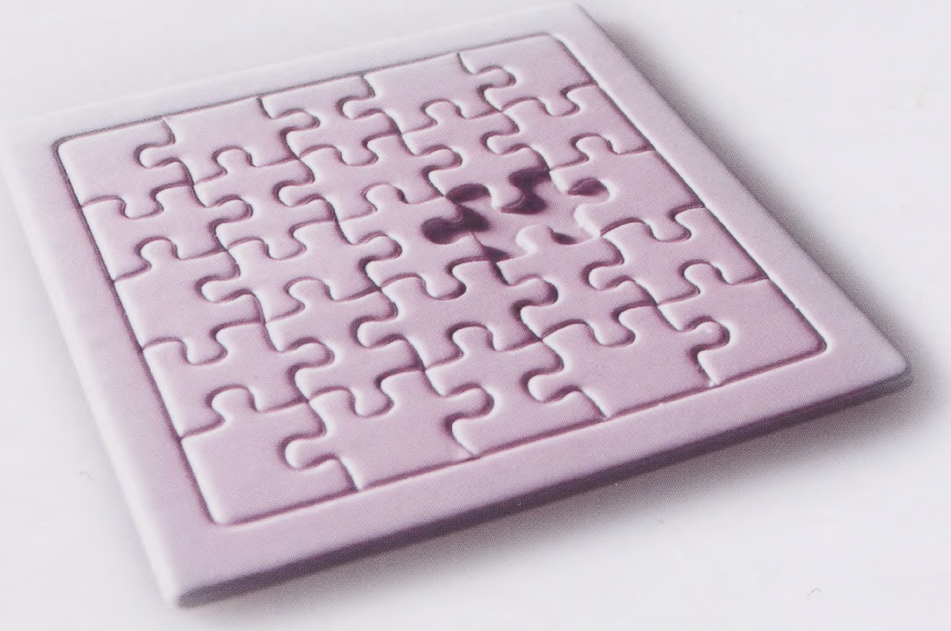
Eternal Challenges

The great conundrums of mathematics



Everything is mathematical

Eternal Challenges

Eternal Challenges

The great conundrums of mathematics

Joaquín Navarro

Everything is mathematical

© 2010, Joaquín Navarro (text)
© 2013, RBA Contenidos Editoriales y Audiovisuales, S.A.U.
Published by RBA Coleccionables, S.A.
c/o Hothouse Developments Ltd
91 Brick Lane, London, E1 6QL

Localisation: Windmill Books Ltd.
Photographs: Corbis

All rights reserved. No part of this publication can be
reproduced, sold or transmitted by any means without
permission of the publisher.

ISSN: 2050-649X

Printed in Spain

Contents

Preface 9

Chapter 1. Great Problems from Antiquity 11
The impossible problem 11
A Greek problem with an oracle and everything 15
Another classic problem, with no oracle and no solution 17
The original theorem 21
There are infinite prime numbers 23
Perfect numbers 25
The sphere and the cylinder 29
The marvellous cycloid 32
Why do honeycombs have hexagonal cells? 37
Kepler and the oranges 38

Chapter 2. A Journey Through the Euler Universe 43
The problem that didn't interest Sherlock Holmes 43
The Basel problem 48
Goldbach's conjecture 52
The three-body problem 56
Legendre's conjecture 58
An elusive brick 61
The bridges of Königsberg 63
A 19-year-old genius 66
In search of the lost equation 69
The prime number theorem 73
And the journey does not end there 77

Chapter 3. Mathematics Comes of Age 81
The most famous conjecture 81
The death of a travelling salesman 86
Four colours suffice 87
Prime pairs 90
The Bieberbach conjecture 94
The 100,000-dollar conjecture 95

Timber! Timber! More timber! 96
  Tait's conjecture 98
  Catalan's conjecture 98
  The prime magic squares conjecture 98
  And one final problem 99

Chapter 4. Hilbert's Problems 101
Problem 1 101
Problem 2 106
Problem 3 108
Problem 4 108
Problem 5 108
Problem 6 108
Problem 7 109
Problem 8 109
Problem 9 109
Problem 10 110
Problem 11 110
Problem 12 111
Problem 13 112
Problem 14 113
Problem 15 113
Problem 16 113
Problem 17 114
Problem 18 115
Problem 19 116
Problem 20 116
Problem 21 118
Problem 22 119
Problem 23 120

Chapter 5. The Clay Problems 121
P versus *NP* 123
The Hodge conjecture 129
The Poincaré conjecture 131
The Riemann hypothesis 138

The green fields of Yang-Mills 144
Unsolvable equations 146
The mother of all conjectures 148

Epilogue 151

Bibliography 153

Index 155

Preface

> *All I know is that I know nothing.*
> Socrates

How do we distinguish a great problem from merely a problem? Let's take an example. A.C. Aitken, a well-known Edinburgh professor, offered to calculate the quotient of 4/47 to several decimal places during a discussion with his colleagues. Aitken began to recite: "0.085106382..." and so on to 26 decimal places. He paused for a few moments and then recited the period to the end without hesitating – a total of 46 digits, one after the other. "Then, the period repeats. If there are 46 digits, that means I'm right." His fellow mathematicians quickly confirmed that he was. However, while this was a spectacular display of Aitken's renowned abilities of mental calculation, it is *not* a 'problem'. Given time (perhaps a lot) and a pencil (or several), anyone could solve it.

Is there a classification of problems? Generally speaking, the answer is no. However, there are criteria, chief among them 'significance'. This is the influence that solving a problem has had on the development of science or the influence it is thought that the solution would have were it to be solved. However, this criterion is difficult to apply in a text like this, since there are problems that at the time must have seemed important and their solution really did constitute a landmark in thought, but are rather basic in modern terms. For example, take the statement 'There are infinite prime numbers' which is absolutely fundamental and incredibly important. In the 21st century, it is formulated in secondary schools. This solution appears in Euclid's *Elements*, written in c. 300 BC, so it might be tempting to assume that it is ancient, as well as basic, and not worth discussing here. Would that be the right approach? This milestone in thought comes under the heading of number theory, a leading discipline as far as problems are concerned. Its problems are easy to formulate and understand and relate to a concept that is relevant to us – but they are genuinely difficult.

Take another problem, this time expressed in modern language: 'Let A be a projective complex manifold. Then every Hodge class on A is a linear combination with rational coefficients of the cohomology classes of the complex subvarieties of A.' What can we say about this so far unsolved problem? In truth, it's hard to know what to say, but not because the question is or is not significant – in fact, the Clay Mathematics Insitute is offering a million dollars to whoever solves it – but rather because it may be incomprehensible to the uninitiated. This book aims to explain the world of mathematics and make it accessible to non-specialists, and we decided that reproducing the incomprehensible should not be one of its goals.

The great problems of mathematics is exactly that – great problems. Unfortunately, they are often incomprehensible if you are not fluent in the language they are written in, a language that people who have spent years learning it might have a fair mastery of, but unfortunately has little in common with the everyday.

An obvious temptation is to focus on a round number of problems, to make a list of say a hundred. However, the result is a contrived and unfair list. The sensible approach is to base our decisions on a global consensus and regard important problems as those that the majority agree are important. This solution does not deliver groundbreaking results, but does guarantee something very worthwhile – we don't make a fool of ourselves. Moreover, thanks to the Internet, the scale of the task is humanly possible, and we can legitimately tailor the size of the book to our readers. The Internet is there for anyone who would like more information. We'll follow the wise majority verdict, and also try to make it clear why a problem is important.

Nevertheless, don't underestimate the task. Michael Barnsley (b. 1972) applied affine transformations to various fractal patterns and in so doing solved a redundancy problem that made possible the small matter of compressing a film on to a single DVD; it also made him a millionaire. Does solving this problem merit inclusion in our list?

Chapter 1

Great Problems from Antiquity

If I have seen further,
it is by standing upon the shoulders of giants.
Sir Isaac Newton

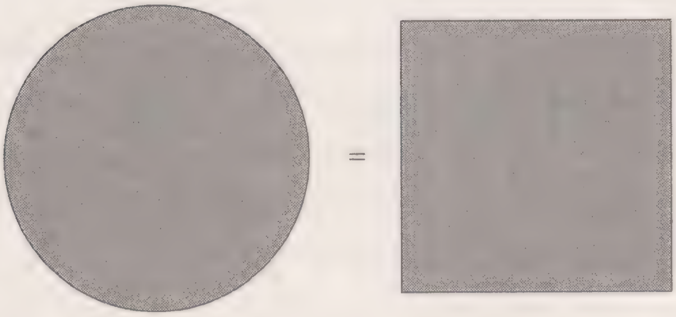
Many of the great mathematical problems mankind has set itself come from antiquity, and especially, due to its intellectual influence, from the Classical Greek era. Today, most of these problems have been solved, but not all of them. Mentioning them is in no sense a concession to history, but rather a rewarding intellectual exercise since, to paraphrase Newton's apt expression above, we are who we are because we have stood on the shoulders of giants.

We respect the achievements of our ancestors; they indicated the path we should follow. Take, for example, the case of prime numbers. It seems appropriate to wonder at the supposed infinite number of prime numbers of the form $2^{2^n}+1$, but first we have to prove that there are infinite primes, and that is not easy. Euclid demonstrated it, but you try to demonstrate it yourself – showing your full workings. You'll learn to respect Euclid, who was never awarded a doctorate or a Nobel Prize, but was very, very smart.

What follows below is a short demonstration of the meaning of the word 'progress'.

The impossible problem

The expression 'to square the circle' has become synonymous with trying to do the impossible. Why? Squaring the circle means finding a square with the same area as a given circle, a problem that people in ancient civilisations had eminently practical reasons for trying to solve. This problem, along with approximate solutions, can be found both in the Bible and in ancient Egyptian and Babylonian texts.



A circle and a square of equivalent areas.

Let's identify a systematic nomenclature so we can focus on the ideas. This was the approach taken in ancient Greece and we'll replicate it here, while updating the explanations a little. We call π the mathematical constant produced by dividing the circumference l of a circle by its diameter d:

$$\pi = \frac{l}{d},$$

and the mathematical constant produced by dividing the area a of a circle by the square of the radius r (which is half the diameter):

$$\pi = \frac{a}{r^2}.$$

The mathematical constant is always the same. We owe this to Archimedes, who demonstrated precisely and irrefutably all three things – that π was a constant and the two formulae above. If we want to square the circle, we have to find the side L of a square with an area a:

$$a = \pi r^2 = L^2 \Rightarrow L = \sqrt{\pi r^2} = r\sqrt{\pi},$$

which means we have to geometrically construct $\sqrt{\pi}$, which is the same as constructing π.

We also have Archimedes to thank for developing a serious method of tackling π. The Greek mathematician tried to calculate it and did so in a very ingenious yet fairly approximate way, never claiming to have calculated it precisely but achieving a magnificent result for the time:

$$3 + 10/71 < \pi < 3 + 1/7.$$

Archimedes arrived at this result using the method of exhaustion, which we owe to the fertile imagination of the mathematician Eudoxus of Cnidus (c. 390

THE ORIGIN OF π

Leonhard Euler (1707–1783) is usually credited with naming π, but in fact he merely endorsed a notation that was first used by William Jones (1675–1749) and was just the first letter of the Greek words περιφέρεια (circumference) and περίμετρος (perimeter).

William Jones, self-taught British mathematician who proposed the use of the symbol π.

–c. 337 BC). Inscribed and circumscribed regular polygons are drawn inside and outside the circumference, their perimeters are calculated and, as sides are added to the polygons, their perimeters approach the actual value of the circumference. In this way π is approximated and limits are set for its supposed exact value.

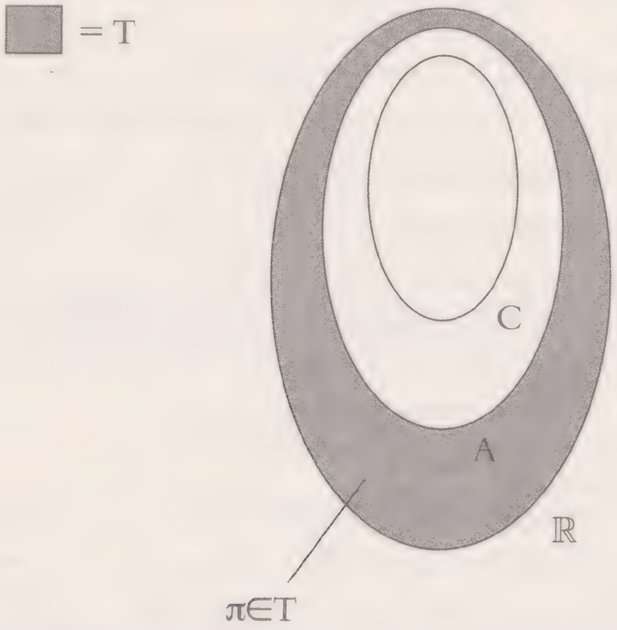
In fact, the exact value would never be found, but the early devotees of π were not to know this. This was the beginning of an unparalleled intellectual odyssey, a quest to square the circle that would not stop even after the announcement in 1753 by the Paris Academy that it would not accept any more alleged proofs for examination. Nor did it stop when Carl Louis Ferdinand von Lindemann (1852-1939) stated that squaring the circle was impossible. It is a strange situation because despite the existence of an irrefutable mathematical proof that a given task is impossible, the visionaries still have enough energy to dedicate to proving it. The author even had to judge one of these 'demonstrations' in the mid-20th century. And, of course, it was mistaken almost from the first page, of which there were some 200.

Purely geometric methods gave way to more powerful and abstract analytical methods, which in turn gave way to methods requiring computers, to whose power we must now bow. But that does not mean that people are now trying to square the circle; that all finished with Lindemann and there is no going back. What is being calculated now is the value of π to so many decimal places, and progress is being made (in 2009 it had been calculated to over 2,699 billion) in search of clues to the normality of π (a term relating to number theory) and its computational complexity.

The following table presents a brief summary of the milestones in the eventful history of π, purely for information purposes.

Date	Protagonist in the event	Approximations of π
c. 2000 BC	Egypt: Rhind Papyrus	$(16/9)^2 = 3.160493...$
c. 1900 BC	Babylonian specialists	$25/8 = 3.125$
c. 900 BC	India: *Shatapatha Brahmana*	$339/108 = 3.138888...$
c. 250 BC	Archimedes	$223/71 < \pi < 22/7$ $(3.140845... < \pi < 3.142857...)$
5	Liu Xin	3.154
150	Ptolemy	$377/120 = 3.141666...$
480	Zu Chongzhi	$3.1415926 < \pi < 3.1415927$
499	Aryabhata	$62{,}832/20{,}000 = 3.1416$
800	Al Khwarizmi	3.1416
1150	Bhaskara	3.14156
1220	Fibonacci	3.141818
1400	Madhava of Sangamagrama using a power series	11 decimal places
1596	Ludolph van Ceulen	20 decimal places
1615		32 decimal places
1621	Willebrord Snell	35 decimal places
1699	Abraham Sharp	71 decimal places
1706	John Machin	100 decimal places
1719	Thomas Fantet de Lagny (calculated 127 decimal places, but they weren't all correct)	112 decimal places
1794	Jurij Vega (calculated 140 decimal places, but they weren't all correct)	137 decimal places
1841	William Rutherford (calculated 208 decimal places, but they weren't all correct)	152 decimal places
1844	Zacharias Dase and Schulz von Strassnitzky (calculated 205 decimal places, but they weren't all correct)	200 decimal places
1847	Thomas Clausen (calculated 250 decimal places, but they weren't all correct)	248 decimal places
1853	William Rutherford	440 decimal places
1874	William Shanks (calculated 707 decimal places, but they weren't all correct)	527 decimal places
1949	D.F. Ferguson and John Wrench, using a desktop calculator	1,120 decimal places
1949	John W. Wrench Jr. and L.R. Smith, using ENIAC, an electronic computer, as is the case with all subsequent researchers.	2,037 decimal places
1958	François Genuys	10,000 decimal places
1961	Daniel Shanks and John Wrench	100,265 decimal places
1973	Jean Gilloud and Martin Bouyer	1,001,250 decimal places
1983	Yasumasa Kanada, Yoshiaki Tamura and Sayaka Yoshino	16,777,206 decimal places
1987	Yasumasa Kanada, Yoshiaki Tamura and Yoshinobu Kubo	134,214,700 decimal places
1989	Gregory V. Chudnovsky and David V. Chudnovsky	1,011,196,691 decimal places
2009	Fabrice Bellard	2,699,999,990,000 decimal places

The problem of squaring the circle has its roots in the Greek concept of constructibility. In principle, the only accepted tools of geometric construction are the ruler and the compass – and then only with certain caveats. This produces a category of numbers that can be represented geometrically. They are called constructible numbers. It is quite easy to demonstrate that any constructible number is also algebraic, although this is a broader category that includes constructible and non-constructible numbers. Defining algebraic numbers seems a little whimsical and off-subject – although it is not – and we only mention it here to tie up the loose ends. A number is algebraic when it is the solution to any equation with rational coefficients. Non-algebraic numbers – a vast, innumerable, uncountable, infinite category – are referred to as transcendental numbers, a historic name deriving from the way they 'transcend' and go beyond algebraic numbers.



Venn diagram showing the relationship between constructible, algebraic, transcendental and real numbers.

Lindemann proved in 1882 that π was transcendental and not algebraic or constructible, so π cannot be constructed using a ruler and compass.

A Greek problem with an oracle and everything

The question we will consider now appears to be of divine origin, because it involves the Oracle of Delphi – to whom the inhabitants of the Greek island of Delos turned for advice – along with the god Apollo, Plato and, later on, many more people. We should point out before we begin that for the Classical Greeks, producing a geometric construction meant using only a ruler and a compass – and that the number of steps had to be finite and that a graded ruler could not be used (units of measurement could not be marked on the ruler in advance). We will also slightly modernise the notation of the following formulae to make life easier.

The – semi-mythical – story concerns the doubling of the cube. Around the year 430 BC the island of Delos suffered a series of horrific fevers, and its inhabitants, weary of the plague, consulted the Oracle of Delphi in the hope of a cure. The Oracle spoke and seemingly requested that a cube-shaped altar to Apollo be increased in size. In fact, the Oracle wanted them to double it. Obediently, the people doubled the length of the altar; if we use l to refer to the length of the original cube and V for its volume, what they did was to construct another altar of volume

$$(2l)^3 = 8l^3 = 8V,$$

in other words, eight times larger. The fevers continued.

The citizens, already familiar with the enigmatic instructions of the Oracle, who specialised in utterances with double meanings, asked Plato to enlighten them. The famous philosopher (and geometer) duly scolded them. What the Oracle had asked them to do was to dedicate to Apollo an altar of twice the volume, not one twice as long. In fact, an altar of length l' and volume V' which satisfied

$$V' = (l')^3 = 2V = 2l^3,$$

or, which amounts to the same,

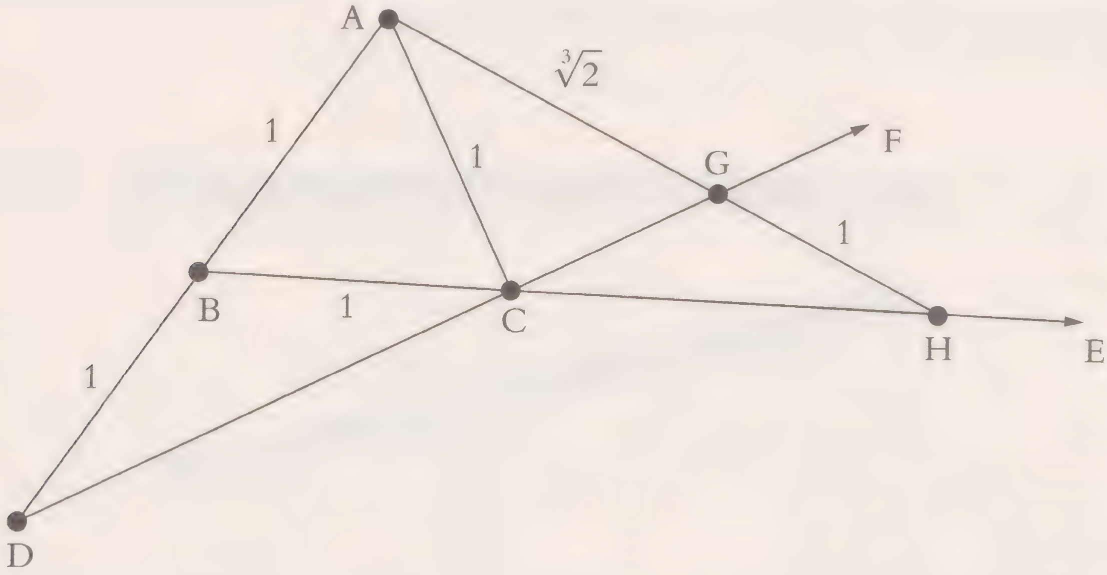
$$l' = \sqrt[3]{2l^3} = l\sqrt[3]{2}.$$

So what Apollo really wanted was for the people of Delos to build him an altar of length $l\sqrt[3]{2}$, an altar that was larger, but not eight times larger. What's more – Plato told them – what Apollo really wanted, and this from the mouth of the enigmatic Oracle, was for the Delians to take a greater interest in mathematics and improve their rusty geometry.

With the problem explained, we have to assume that the fevers cured themselves or that Apollo decided to end them, because what is now referred to as the Delian problem has no solution – as Pierre Wantzel (1814–1848) proved in 1837.

The Delian problem requires the geometric construction of $\sqrt[3]{2}$ using only a ruler and compass in the Greek style. There are many methods of constructing $\sqrt[3]{2}$ using ruler and compass – see, for example, Archytas (428–347 BC), Menaechmus (380–320 BC), Philo of Byzantium (280–220 BC), Nicomedes (280–210 BC), Diocles

(240–180 BC) and Hero of Alexandria (10–75 AD) – but all involve a prohibited use of the ruler and compass. Even a very clever construction discovered by the great Sir Isaac Newton (1643–1727), shown in the graphic below, requires marking the length of the altar on the ruler.



Numbers constructible with ruler and compass can be grouped in a series of sets (in modern algebra they are referred to as field extensions):

$$K_0 \subset K_1 \subset K_2 \subset K_3 \subset K_4 \subset \ldots \subset K_n \subset \ldots,$$

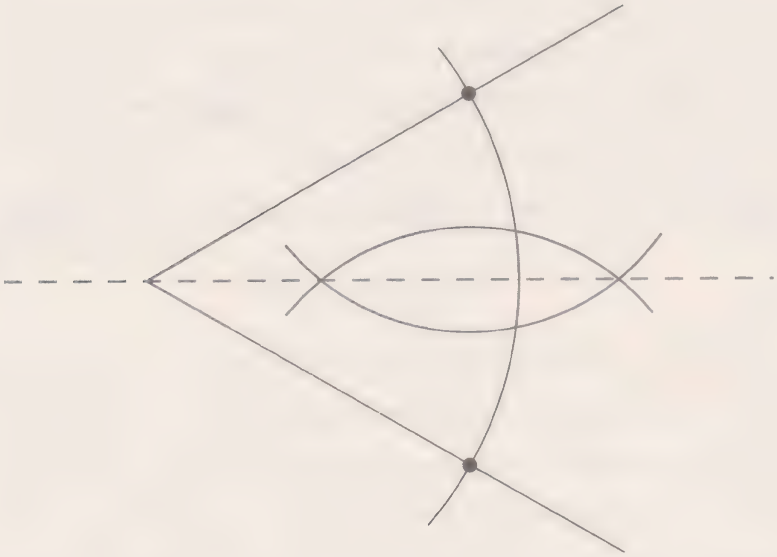
where the members of K_0 are of the form $a_0 + \sqrt{b_0}$; the members of K_1, of the form $a_1 + \sqrt{b_1}$ where $a_1, b_1 \in K_0$ and so on. In K_n the members are of the form $a_n + \sqrt{b_n}$ where $a_n, b_n \in K_{n-1}$. These fields, all made up of constructible numbers, are formed of linear combinations of square roots, linear combinations constructed from the latter (which in reality are quarter roots), octave roots, and so on, but not cube roots.

The altar the Oracle wanted was not constructible because $\sqrt[3]{2}$ is not a square root, nor a quarter root, nor an octave root, nor a root of even order. Indeed, it is not in any telescoping series of fields of the type K_n. Apollo mustn't have known.

Another classic problem, with no oracle and no solution

To trisect an angle is to divide it into three equal parts. In Classical Greece, trisecting an angle meant dividing it in accordance with the rules of the discipline of geometry; in other words, dividing an angle α into three equal parts using only ruler and compass, with the inherent restrictions on these tools that we have already seen. Of course, the application of such strict rules was not a whim but rather a consequence of the quest for maximum perfection and absolute precision. The Greeks shunned crude approximations and trial and error; they sought accuracy.

Their requirements were underpinned by common sense. Many of us know how to bisect an angle, as shown in the illustration below.



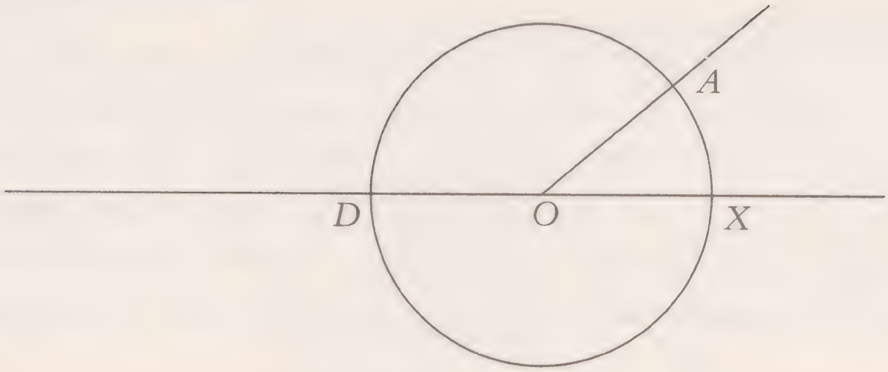
But say we repeat the bisection an infinite number of times. We get successive angles of degree $\alpha/2, \alpha/4, \alpha/8 \ldots, \alpha/2^n \ldots$, and if we add the series

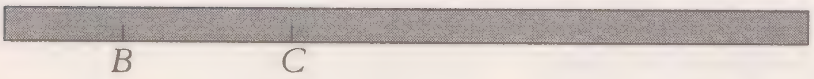
$$\alpha/4 + \alpha/16 + \alpha/64 + \ldots + \alpha/4^n + \ldots = \alpha/3$$

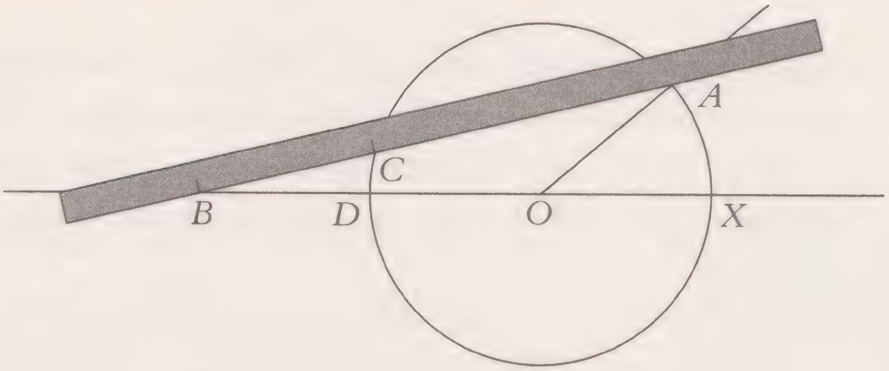
we have trisected α. Except the number of steps is not finite and we have violated the requirement to use ruler and compass. We have also gone against common sense, and we do not recommend that anybody try infinite bisection.

It is also true that some angles can be trisected according to the rules. Readers can try for themselves to trisect angles of degree π, $3\pi/8$, $\pi/6$ or $\pi/4$, for example. It is possible, we assure you, although you might find it difficult. However, the Greeks required a procedure for trisecting any angle, not just one specific angle.

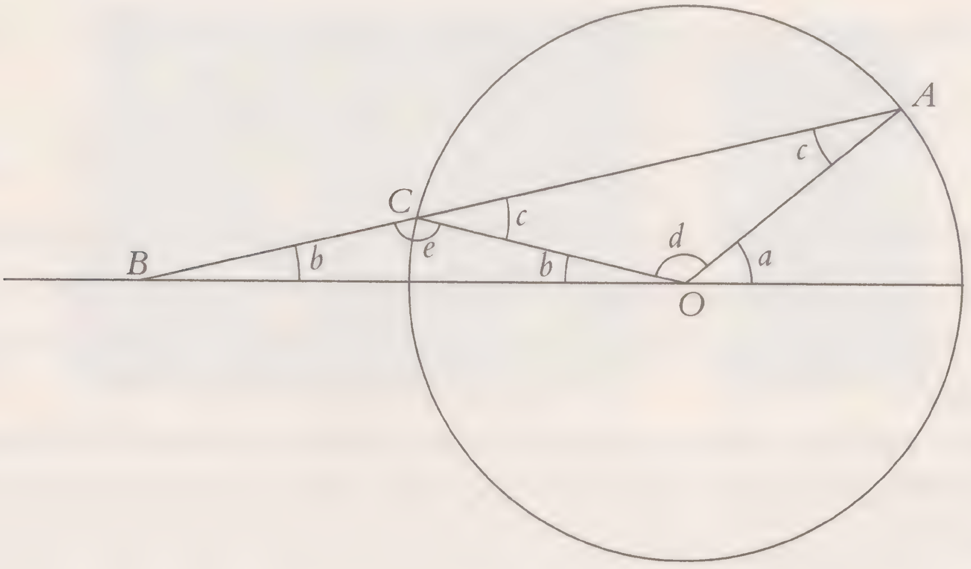
In fact, Archimedes managed to devise a highly ingenious procedure for trisecting any angle; it is a Neusis construction which bends the usual rules and allows the use of a marked ruler. If *AOX* is angle to be trisected, Archimedes stated that if two marks B and C are made on any ruler and the steps in the figures below are followed, *AOX* can be trisected.







The angle *CBD* measures 1/3 *AOX*. This method requires the ruler to be pivoted around *A* until *C* coincides with the circumference and *D*, with the straight line *OX*. It is a very ingenious construction, and adding several more lines and letters to the diagram will help us to understand how it is done.



Note that the following equations hold true:

$$e + c = \pi$$
$$e + 2b = \pi$$
$$c = 2b$$
$$d + 2c = \pi$$
$$a + d + b = \pi$$

Combined neatly, these give $a = 3b$. However, Archimedes' method uses a marked ruler and this is against the rules.

Other prohibited methods, which the Greeks referred to as 'mechanical', were based on using, for a trisection, pre-existing curves called trisectrices. This term is used for all curves that can be constructed using a known geometric procedure – usually their equations – and which when used correctly can be used as a reference for trisecting angles.

An analysis of the division of an angle 3α into three equal parts α produces a third-degree equation. In effect, constructing α is equivalent to constructing any of its simplest trigonometric functions, since we are dealing with simple segments. Applying the rules of trigonometry to a composite angle, for example, gives the expression

$$4\sin^3 \alpha - 3\sin \alpha + \sin 3\alpha = 0,$$

which taking $\sin \alpha = x$ gives us the following cubic equation:

$$4x^3 - 3x + \sin 3\alpha = 0.$$

And while there are solvable cubic equations in the world of constructible numbers, and there are trisectable angles (as Cardano taught us, by means of formulae), the solutions generally involve cubic roots. And cubic roots are not constructible.

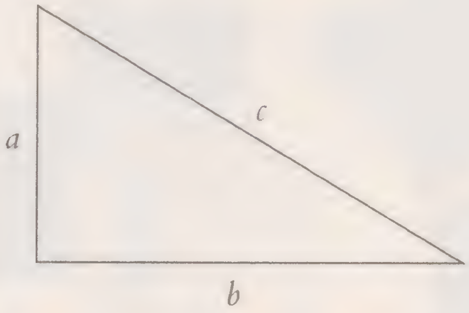
Pierre Wantzel, as in the previous problem (doubling the cube) and in the same text of 1837, definitively resolved the problem at the age of 23 by producing a negative solution. Angle trisection is generally impossible using ruler and ruler.

The original theorem

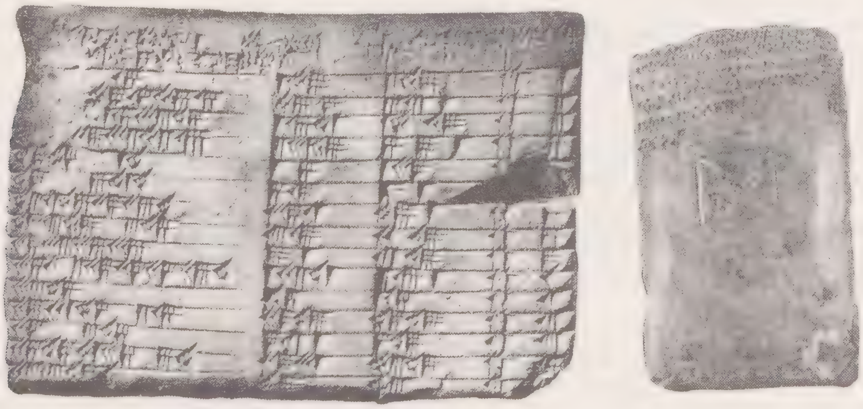
'The sum of the squares of the legs of a right-angled triangle is equal to the square of the hypotenuse' is the first geometric theorem we are taught in school, and also one of the first complex questions to occupy the human mind in its analysis of the natural world. And so began the history of science.

In any right-angled triangle with legs a and b (the legs are the sides adjacent to and opposite to the right angle), and hypotenuse c (the remaining side) it holds true that

$$a^2 + b^2 = c^2.$$

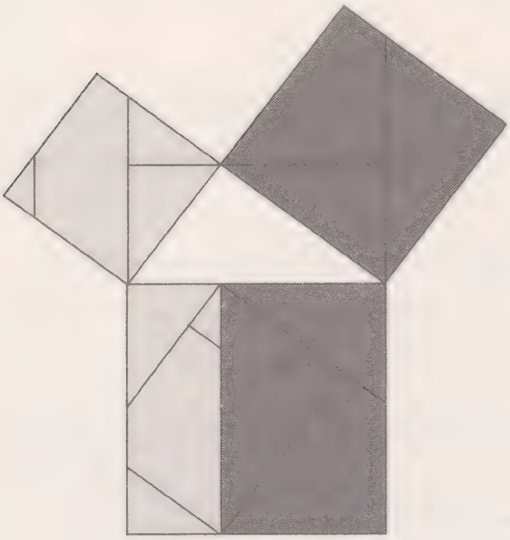


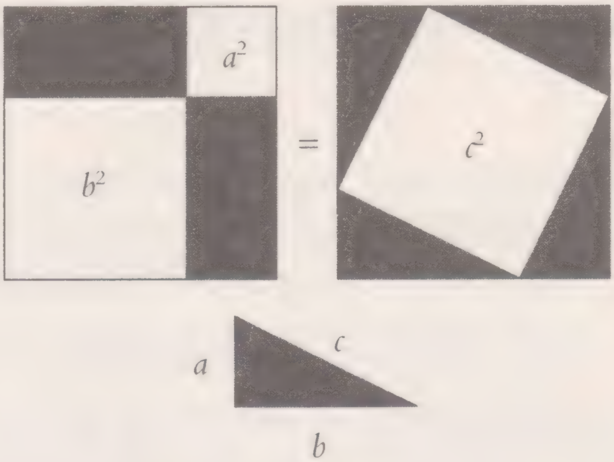
Reciprocally (reciprocal theorem), if a, b and c fulfil these conditions, the triangle is a right-angled triangle. History, or more correctly legend, credits the discovery to the philosopher and mathematician Pythagoras of Samos (c.a. 582–507 BC), although it is almost certain that he did not prove it himself, since it was common for discoveries made by a school of philosophy to be attributed to the head of the school. Furthermore, it is doubtful whether Pythagoras or the Pythagorean school could claim absolute ownership of the theorem, since it appears that the Babylonians knew of the formulation, and perhaps the Egyptians too.



The Babylonian tablet Plimpton 322 (left), carved between 1790 and 1750 BC, shows various groups of three Pythagorean numbers, suggesting a good knowledge of the so-called Pythagoras' theorem. The Mesopotamian civilisation applied it to practical geometric questions, such as calculating the sides of a square field based on the diagonal, as shown in the tablet on the right.

Nonetheless, the first person to prove the theorem was Euclid of Alexandria (ca. 300 BC) in his *Elements*, 'Book I', Proposition 47. There are dozens of subsequent proofs of all kinds, including some that use, strangely enough, concepts as abstract as differential equations. The most striking demonstrations, those that do not require the reader to perform any calculation to appreciate them, are perhaps the two shown here in the following diagrams.





The groups of three numbers a, b and c which satisfy, for any given natural integer x and y, the following conditions

$$a = x^2 - y^2$$
$$b = 2xy$$
$$c = x^2 + y^2$$

are given the historic designation Pythagorean, since $a^2 + b^2 = c^2$. The equations also hold true for any type of number.

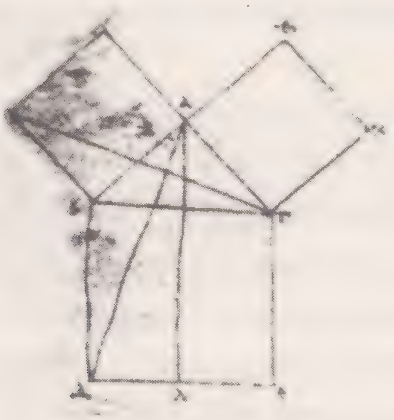
And since we are on the subject of types of numbers, it is worth noting that the apparently inoffensive and beautiful Pythagoras' theorem caused all sorts of problems for the Pythagoreans themselves. If applied to the diagonal of a square with rational side lengths L, the diagonal measures

$$D = \sqrt{L^2 + L^2} = \sqrt{2L^2} = L\sqrt{2},$$

which is not rational. The Greeks termed such numbers 'incommensurable', but we use 'irrational' today. The Pythagoreans could not conceive of a number that was not commensurable and legend has it that Hippasus of Metapontum, who made the discovery, was executed for revealing the existence of irrational numbers. A less gruesome version has it that Hippasus was merely expelled from the cult-like Pythagorean community.

The Pythagorean relationship $a^2 + b^2 = c^2$, equivalent to $c=\sqrt{a^2+b^2}$, was subsequently interpreted as a definition of the Euclidean metric, which postulates that an n-dimensional space is Euclidean if it features a distance:

$$d=\sqrt{(x_1-y_1)^2+...+(x_n-y_n)^2}.$$



An image of a very old Greek version of Euclid's Elements
showing the diagram that accompanied the demonstration of Pythagoras' theorem.

There are infinite prime numbers

This statement may seem commonplace today, but for Euclid's contemporaries it certainly wasn't. It appears as a theorem, fully demonstrated, in "Book IX", Proposition 20, of the *Elements*. It also appears in any basic arithmetic textbook as a fundamental law. Remember that a natural number, $n > 1$, is prime if it has no positive divisor other than itself. According to this definition, 1 is not prime. Non-prime numbers are called composite numbers. The prime numbers under 100 are:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

There is an algorithm, as slow as it is infallible, for calculating them called the Sieve of Eratosthenes. The first question that occurs to us on seeing the series above is – is there an end to it? The answer, contained in Euclid's treatise, is a miracle of reasoning so incredible that it is still used as a model today. Let's go through it. We'll take a finite series of consecutive prime numbers, 2, 3, 5, 7…, p and generate the new number $n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot p + 1$, which will either be prime or composite (a product of prime numbers). Let's take the first option and assume that n is prime. It's obvious that $n > p_i$, where p_i is any prime number from the previous sequence. Therefore, we have generated a new and larger prime number. So, if n were still prime, we would have finished already.

Let's take the second option and assume that n is composite. Now there are two alternatives:

1. None of its prime factors is greater than p.
2. One of its prime factors is greater than p.

Consider the first alternative. One of the factors of n must be one of the prime numbers from the sequence 2, 3, 5, 7…, p; we'll call it m. So m divides n and, because it is prime, m divides the product $2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot p$. If it divides both numbers, then it also divides the difference between the two, $n - 2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot p = 1$. So the number m, divides 1, and therefore $m = 1$. But this number is not in the sequence 2, 3, 5, 7…, p so our initial assumption is not true; it is untenable.

The second alternative must therefore be true. If there were a prime factor of n greater than p, we would have discovered the Egg of Columbus, since given the prime p there is always a larger prime number. We will never stop discovering increasingly large prime numbers. We can conclude, therefore, that the sequence of prime numbers is infinite.

Euclid drawing, as depicted by Raphael in his monumental work The School of Athens.

Euclid's brilliant demonstration may seem a little long, convoluted and, in order to simplify matters, at times formulated a little hastily, which can give rise to various misunderstandings.

For example, rushed readers might conclude that if

$$n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot p + 1$$

n is, obviously, prime, since when dividing it by any of 2, 3, 5, 7…, p it gives the remainder 1. In fact, we can only conclude that if n is composite, the smallest of its prime factors must be greater than p. The example usually given to demonstrate this is the prime decomposition

$$(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) + 1 = 30{,}031 = 59 \cdot 509.$$

The largest prime number known in 2012 was $2^{43,112,609} - 1$, which has 12,978,189 digits. It may soon be exceeded, firstly because there are infinite prime numbers and the eagerness to go further is also infinite, and secondly because the Electronic Frontier Foundation has offered a reward of 150,000 dollars to the first person to find a 100,000,000-digit prime number (base 10, of course).

It should be borne in mind that prime numbers are the engine of a whole branch of mathematics, number theory, and the most frequent protagonists of the great problems and discoveries of mathematics as a whole. To conclude, this theorem ('there are infinite prime numbers') might be regarded as *the* theorem, the most powerful possible assertion about these numbers. But it isn't. The gloriously named *prime number theorem* makes another claim about them, not demonstrated until the late 19th century, as we will see later.

Perfect numbers

It is often said that perfection is otherworldly, but perhaps it can be found in the world of numbers; indeed there has been a passion for perfect numbers since the time of Pythagoras and his followers. This passion may well have extended beyond Greece, because it seems perfect numbers also interested the Egyptians.

They are defined as follows: a number is perfect when it is equal to the sum of its own positive divisors (except the number itself, naturally). For a practical definition of these numbers, the function $\sigma(n)$ was devised, which is equivalent to the sum of the divisors of n (careful, now we are including n itself). A number, then, is perfect when $\sigma(n) = 2n$.

When we start looking for them, we soon realise that the equation holds true with a certain degree of ostentation. Perfection is scarce, as shown in the following table, which compares the respective sizes of n, the perfect number P_n nth and the prime number p_n which generates it:

n	p_n	P_n
1	2	6
2	3	28
3	5	496
4	7	8,128
5	13	33,550,336
6	17	8,589,869,056
7	19	137,438,691,328
8	31	2,305,843,008,139,952,128

And it's a good thing we stop there. Saint Augustine of Hippo believed that God created the world in six days because 6 is a perfect number. It's as well He didn't create it in any other perfect period, because it would have taken Him many more days. By way of example, let's write down here the 15th perfect number, which is still on a human scale:

541625262843658474126544653743913161408564905390316957846039208183
872069941585348591989999210567199219190573900802636461592800138276
054397462627889030573034455058270283951394752077690449244314948617
294351131262808379049304627406817179604658673487209925721905694655
452996299198234310310926242444635477896354414813917198164416055867
880921478866773213987566616247145517269643022175542817842548173196
119516598555535739377889234051462223245067159791937573728208608782
143220522275845375528974762561793951766244263144803134469350852036
575847982475360211728804037830486028736212593137899949003366739415
037472249669840282408060421086900776703952592318946662736152127756
035357647079522501738583051710286030212348966478513639499289049732
921451075059799114562215198993457649842913 28.

As of 2012, the largest known perfect number had 25,956,377 digits. One of its factors is, in fact, the largest known prime number. You'll note that we haven't yet mentioned odd and even perfect numbers, because by chance all the perfect numbers discovered so far are even, even though the search has gone as far as 10^{300}. Indeed, the odd perfect number conjecture suggests that they don't exist. No examples have been discovered yet… It is known, however, that if an odd perfect number should exist it must have at least 47 prime factors (including repetitions).

In his *Elements*, Euclid dedicated considerable space to even perfect numbers and demonstrated, in 'Book IX', Proposition 36, that any perfect number is of the form:

$$P_n = 2^{n-1}(2^n - 1),$$

whenever $2^n - 1$ is prime. This is not too complicated (sharp readers can try to demonstrate it with the help of the function σ), but proving the reciprocal relationship is not as simple. Proving that any number of the form $2^{n-1}(2^n - 1)$ where $2^n - 1$ is prime is a perfect number required the personal intervention of the great Euler in the 18th century.

Curiously, it is worth noting that the previous expression means that when written in binary code *all* perfect numbers take on a repetitive form:

$$\begin{gathered} 6_{10} = 110_2 \\ 28_{10} = 11100_2 \\ 496_{10} = 111110000_2, \end{gathered}$$

made up of p_n ones followed by $p_n - 1$ zeros.

We cannot tell this story without mentioning Father Marin Mersenne (1588-1648), a French theologian, philosopher and mathematician who was also an expert in music and examined numbers of the form

$$M_n = 2^n - 1,$$

conjecturing (and giving a flawed list) that many of them were primes. Mersenne theorised that they were only prime when $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257. But when $n = 61, 89$ and 107, prime numbers are also generated (but were not included in his list) and for 67 and 257 composite numbers are generated (but were included in his list of suspected primes).

So important were his numbers that even Countess Ada Lovelace, daughter of Lord Byron, ended up working on them. In fact, Mersenne primes generate the only even perfect numbers that exist, according to the combined Euclid and Euler method. There are as many Mersenne primes as there are even perfect numbers and vice versa. Research into Mersenne primes (in 2012 47 were known) is still very active. One factor contributing to the popularity of this research is perhaps the fact that finding Mersenne primes means finding very large primes.

We do not yet know whether there is a finite or infinite number of even perfect numbers. It is an unresolved problem. Theoretically there should also be abundant numbers, deficient numbers, harmonic numbers, multiperfect numbers, pseudoperfect numbers, pluperfect numbers, quasiperfect numbers, etc. All of these are related in one way or another to perfect numbers and all come with their own unresolved problems.

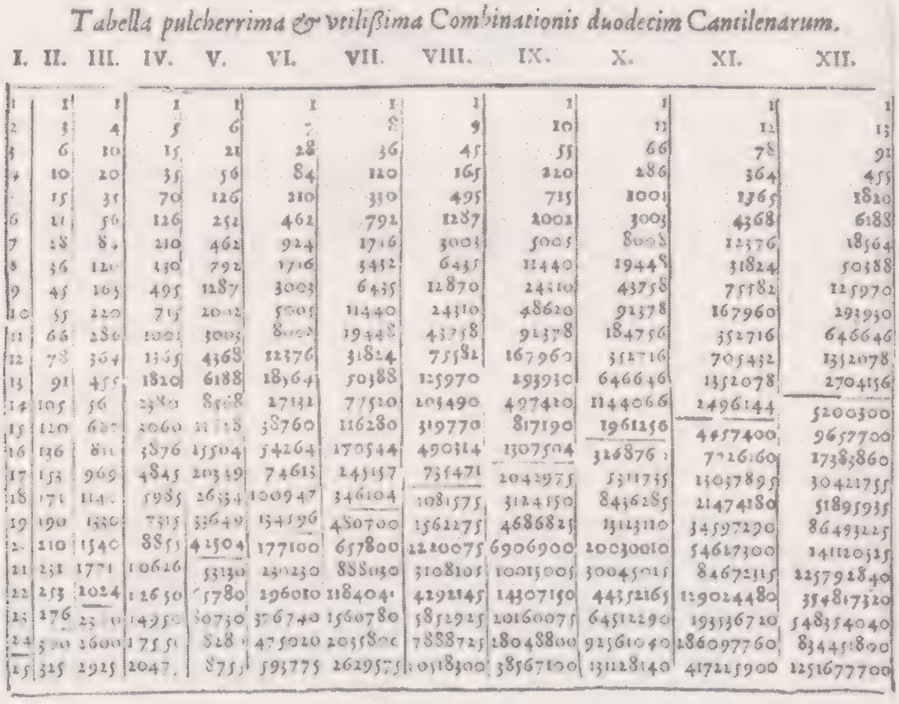


Tabella pulcherrima & vtiliſsima Combinationis duodecim Cantilenarum.

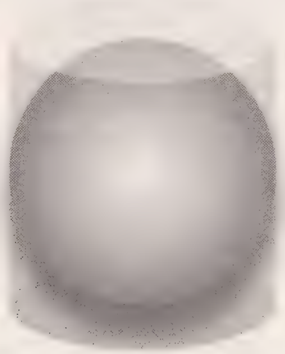
I.	II.	III.	IV.	V.	VI.	VII.	VIII.	IX.	X.	XI.	XII.
1	1	1	1	1	1	1	1	1	1	1	1
2	3	4	5	6	7	8	9	10	11	12	13
3	6	10	15	21	28	36	45	55	66	78	91
4	10	20	35	56	84	120	165	220	286	364	455
5	15	35	70	126	210	330	495	715	1001	1365	1820
6	21	56	126	252	462	792	1287	2002	3003	4368	6188
7	28	84	210	462	924	1716	3003	5005	8008	12376	18564
8	36	120	330	792	1716	3432	6435	11440	19448	31824	50388
9	45	165	495	1287	3003	6435	12870	24310	43758	75582	125970
10	55	220	715	2002	5005	11440	24310	48620	92378	167960	293930
11	66	286	1001	3003	8008	19448	43758	92378	184756	352716	646646
12	78	364	1365	4368	12376	31824	75582	167960	352716	705432	1352078
13	91	455	1820	6188	18564	50388	125970	293930	646646	1352078	2704156
14	105	56	2380	8568	27132	77520	203490	497420	1144066	2496144	5200300
15	120	680	3060	11628	38760	116280	319770	817190	1961256	4457400	9657700
16	136	816	3876	15504	54264	170544	490314	1307504	3268760	7726160	17383860
17	153	969	4845	20349	74613	245157	735471	2042975	5311735	13037895	30421755
18	171	1140	5985	26334	100947	346104	1081575	3124550	8436285	21474180	51895935
19	190	1330	7315	33649	134596	480700	1562275	4686825	13123110	34597290	86493225
20	210	1540	8855	42504	177100	657800	2220075	6906900	20030010	54627300	141120525
21	231	1771	10626	53130	230230	888030	3108105	10015005	30045015	84672315	225792840
22	253	2024	12650	65780	296010	1184040	4292145	14307150	44352165	129024480	354817320
23	276	2300	14950	80730	376740	1560780	5852925	20160075	64512290	193536720	548354040
24	300	2600	17550	98280	475020	2035800	7888725	28048800	92561040	286097760	834451800
25	325	2925	20475	118755	593775	2629575	10518300	38567100	131128140	417225900	1251677700

Father Marin Mersenne made significant contributions to the fields of mathematics and music, two closely linked disciplines. The illustration shows one of the tables from his work on harmonics.

A subspecies of perfect numbers are amicable numbers. *n* and *m* are amicable when their respective divisors – except the numbers themselves – add up to the other. When a number is amicable with itself, it is perfect, and vice versa. Of course, two numbers can be amicable without being perfect. For example, the pair (9,363,584 and 9,437,056) is formed by two amicable numbers, of which there are an infinite number, according to the work of Thabit ibn Qurra (826-901), who discovered a system for calculating them (not all of them). The path of friendship continues with sociable numbers, which are generalisations of amicable numbers. But there is no reason to believe that everything is friendly, at least in the world of numbers. There are no known sociable numbers of order three.

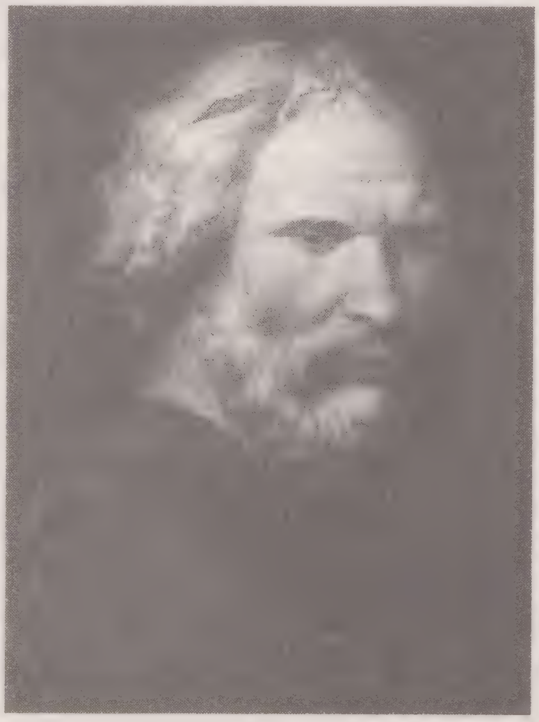
The sphere and the cylinder

Archimedes of Syracuse (287–212 BC) was the first to prove that a sphere has two-thirds the area and volume of its circumscribing cylinder. The diagram below helps us to visualise this:



THE PRIDE OF ARCHIMEDES

When calculating the area of a cylinder, the area of the bases has to be included. Archimedes was so proud of solving this problem that, according to the historian Plutarch, he asked for it to be written on his tomb, an unheard-of tribute for a genius of his calibre. While the tomb is no more, his wishes may well have been carried out. There is testimony to support it from a notable visitor to Archimedes' grave, the famous Roman citizen Marcus Tullius Cicero.

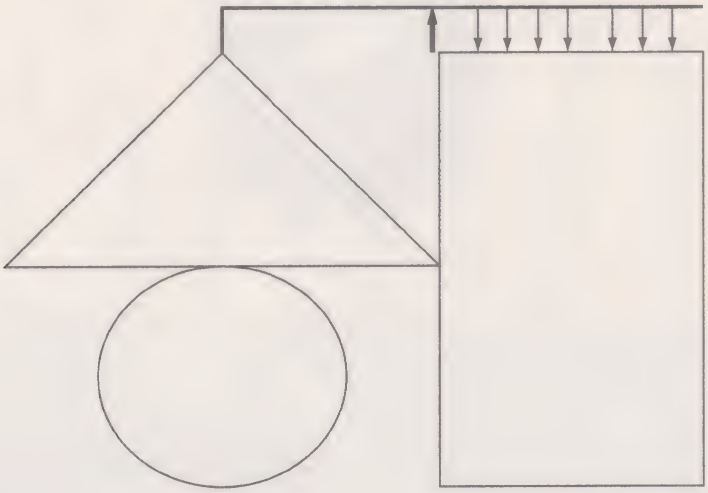


Archimedes, in an imaginary portrait by Giuseppe Catania from the 19th century.

In modern notation, Archimedes' assertion is equivalent to saying that

$$A = 4\pi r^2 \qquad V = \frac{4}{3}\pi r^3$$

are the expressions of the area and volume of a sphere. It seems proving this result was no easy task, since it is meticulously demonstrated in *On the Sphere and the Cylinder*, a major work with 53 propositions. In 1906, Helberg, a Dane, discovered an ancient scroll with a collection of Orthodox Greek prayers written over an older text, Archimedes' *Method of Mechanical Theorems*, which had hitherto been thought lost (it sold for \$2,000,000 in 1998). In this palimpsest, the area and volume of the sphere are expressed using mechanical speculations that draw on the great Greek engineer's particular knowledge of levers.



A lever balancing three geometric bodies with fixed measurements. In Archimedes' work The Method of Mechanical Theorems, *a reasoning based on a similar lever leads him to calculate the area and volume of the sphere.*

Nonetheless, the proof of the previous formulae is derived from the method of exhaustion, discovered by Eudoxus and regarded as a precursor of modern infinitesimal calculus. The method of exhaustion now states, in the more modern and comprehensible terms of limits, that if a quantity A_n is systematically reduced and increased

$$x_n \le A_n \le y_n$$

then the following also holds true

$$\lim_{n\to\infty} x_n \le \lim_{n\to\infty} A_n \le \lim_{n\to\infty} y_n,$$

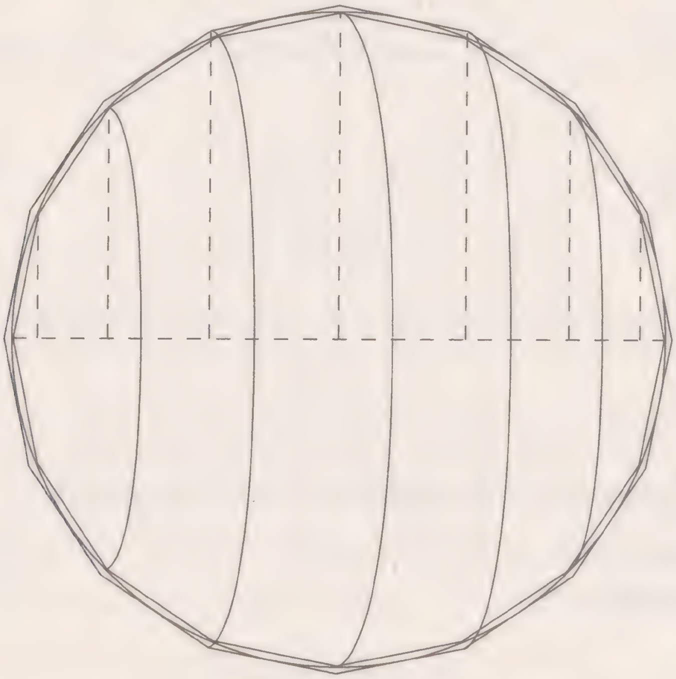
and if the distance between x_n and y_n tends towards zero,

$$\lim_{n\to\infty} (x_n - y_n) \to 0,$$

then the limits are all equal:

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} A_n = A = \lim_{n\to\infty} y_n.$$

What Archimedes did was to inscribe and circumscribe a series of conic sections inside and outside the sphere so that he could calculate both (inscribed and circumscribed) areas and volumes, which gradually tend towards the same value, as can be seen in the illustration below.



Today, intelligent and well-informed schoolchildren can use integral and differential calculus, but in Archimedes' time this obviously wasn't possible. The methods of calculus used in Greek mathematics were purely geometric and anyone reading *On the Sphere and the Cylinder* will see that they are highly ingenious and insightful. Not for nothing is Archimedes regarded as one of the outstanding figures in the history of thought.

The marvellous cycloid

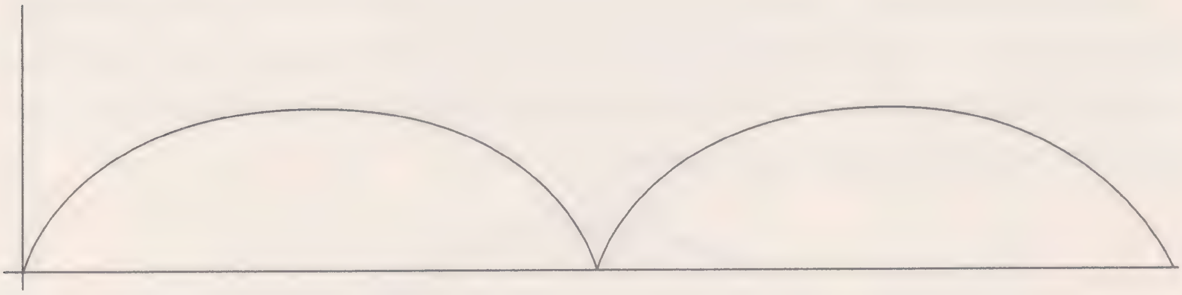
The cycloid looks like any old curve, with the parametric equation

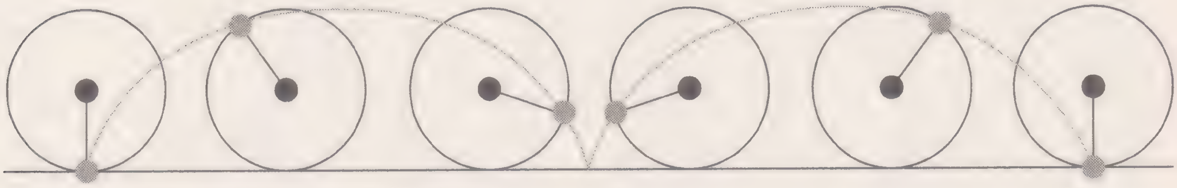
$$x = a\,(\lambda - \sin\lambda)$$
$$y = a\,(1 - \cos\lambda)$$

and the slightly more complicated Cartesian equation

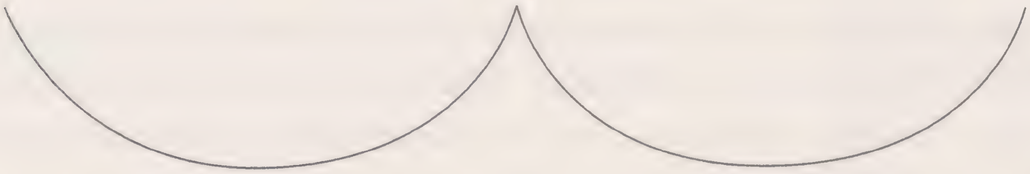
$$x = a \cdot \arccos\,(1 - \frac{y}{a}) - \sqrt{2ay - y^2},$$

where the total height of the curve is $2a$. The length of each period – the period equals 2π – is $8a$, four times the height of the cycloid. The form of the curve is shown in the graph below.



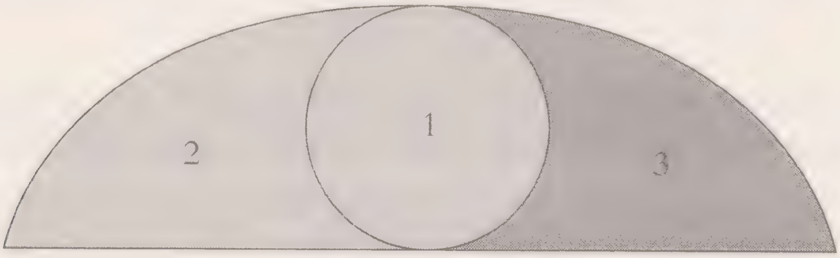


Its geometric definition is already clear from this illustration. A cycloid is the curve traced by a point on the circumference of a rolling circle of radius a. While the hollow points downwards, to illustrate clearly its construction we can also imagine the cycloid facing upwards.



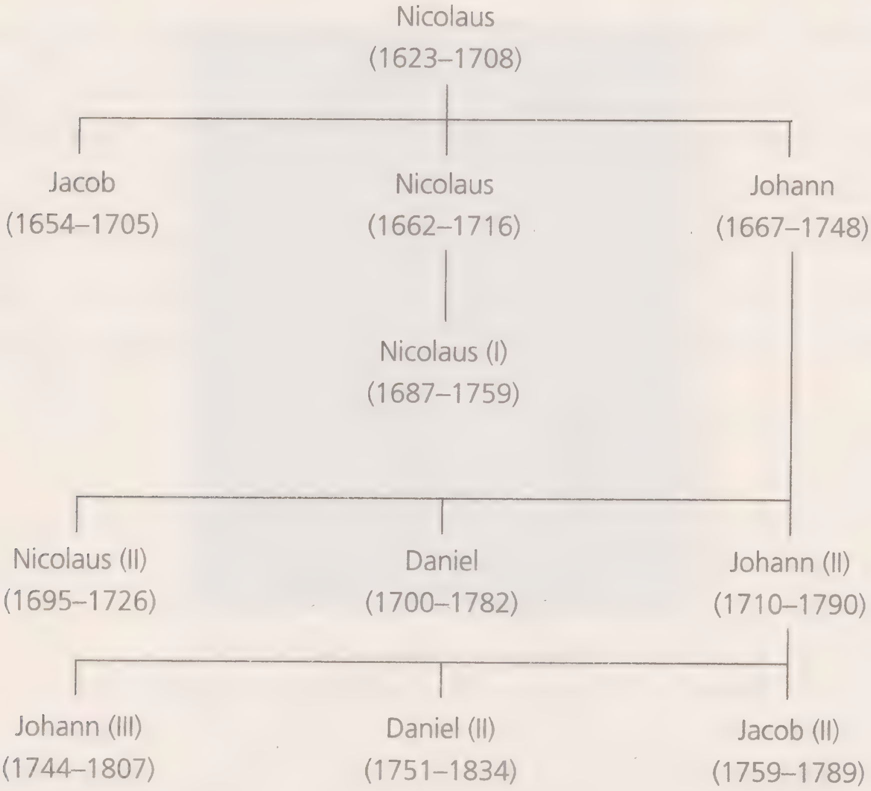
A cycloid with hollow facing upwards.

Among other curiosities, the area inside a cycloid is three times the area of the circle that generates it.



The cycloid and its area.

Now that we have introduced the cycloid, we can introduce the Swiss Bernoulli family:


Nicolaus
(1623–1708)
Jacob
(1654–1705)
Nicolaus
(1662–1716)
Johann
(1667–1748)
Nicolaus (I)
(1687–1759)
Nicolaus (II)
(1695–1726)
Daniel
(1700–1782)
Johann (II)
(1710–1790)
Johann (III)
(1744–1807)
Daniel (II)
(1751–1834)
Jacob (II)
(1759–1789)

The Bernoulli family tree.

Not only were there lots of Bernoullis, they also regularly fell out with each other and had fierce arguments. But this did not prevent them from working together in the field of science. Johann senior, who was a very shrewd thinker – and a dreadful father – discovered the solution to an easily stated but difficult-to-solve problem that would now be described in terms of boundary values, or calculus of variations. It was the following: if we force a mobile particle to move along an inverted curve under its own weight and assuming no friction, what is the curve of most rapid descent? In 1696, Johann Bernoulli published the following text in *Acta Eruditorum*:

> "I invite mathematicians to solve a new problem: given two points *A* and *B* in a vertical plane, and a movable point *M*, find the path *AMB* down which it must by virtue of its own weight proceed from point *A* to point *B* in the shortest possible time. [...] In the meantime, to guard against a rush to judgement, please note that although the straight line *AB* is certainly the shortest path between the points *A* and *B*, it is not, for all that, the path traversed in the shortest time. However, the curve *AMB*, which I shall name, if no person should have discovered it before one year is out, is a curve well known to geometers."

Portrait of Johann Bernoulli, a mathematician whose work focused mainly on infinitesimal calculus.

Galileo Galilei (1564-1642) had already worked – erroneously – on this problem, which might appear to be of little significance but proved to be very relevant as a bridge between physical lucubrations and mathematics. In modern terms,

$$t_{AB} = \int_A^B \frac{ds}{v},$$

where t_{AB} is the time taken to go from point A to B of the curve; s gives the arc of the curve and v, the speed of the particle.

Given that

$$ds=\sqrt{dx^2+dy^2}=\sqrt{\frac{dx^2+dy^2}{dx^2}}dx=\sqrt{1+y'^2}dx,$$

it must be true that

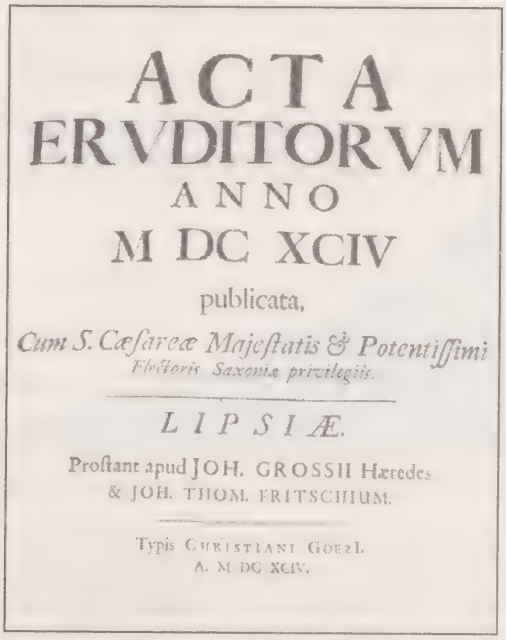
$$t_{AB}=\int_A^B\sqrt{\frac{1+y'^2}{2gy}}dx.$$

The application of variational principles to this expression gives a curve with the parametric equation in terms of α, which is

$$x=\tfrac{1}{2}K(\alpha-\sin\alpha)$$
$$y=\tfrac{1}{2}K(1-\cos\alpha),$$

which is in fact a cycloid. Naturally, Johann did not yet know the secrets of calculus of variations – elaborated later by Euler based on the ideas of Jacob Bernoulli – and proceeded using his ingenuity and on the behaviour of a refracted ray of light.

As noted above, Johann Bernoulli published the problem in the form of a challenge in 1696 in *Acta Eruditorum*, one of the few scientific journals that existed at the time. Deep down inside, he hoped to humiliate his brother Jacob by setting him a difficult puzzle to solve. One year later, Jacob published a possible solution, but it was flawed.



ACTA
ERVDITORVM
ANNO
M DC XCIV
publicata,
Cum S. Cæſareæ Majeſtatis & Potentiſſimi
Electoris Saxoniæ privilegiis.

LIPSIÆ.

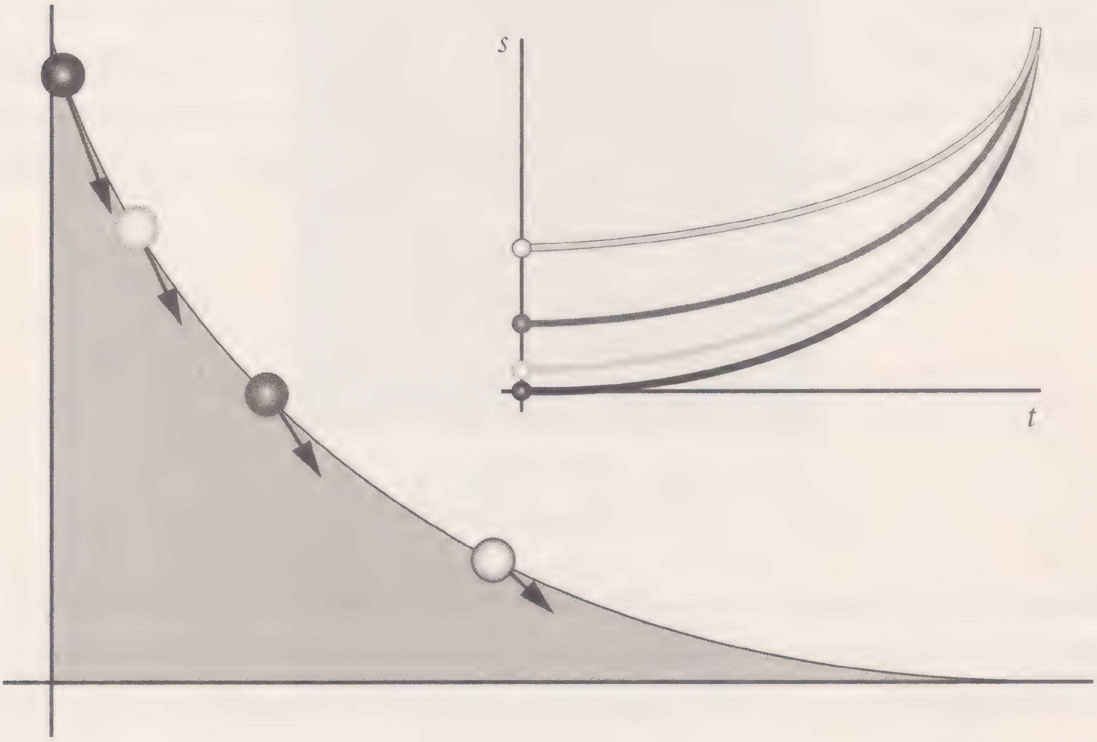
Proſtant apud JOH. GROSSII Hæredes
& JOH. THOM. FRITSCHIUM.

Typis CHRISTIANI GOEZI.
A. M DC XCIV.

Cover page of a volume of Acta Eruditorum, *a German scientific journal published between 1682 and 1782.*

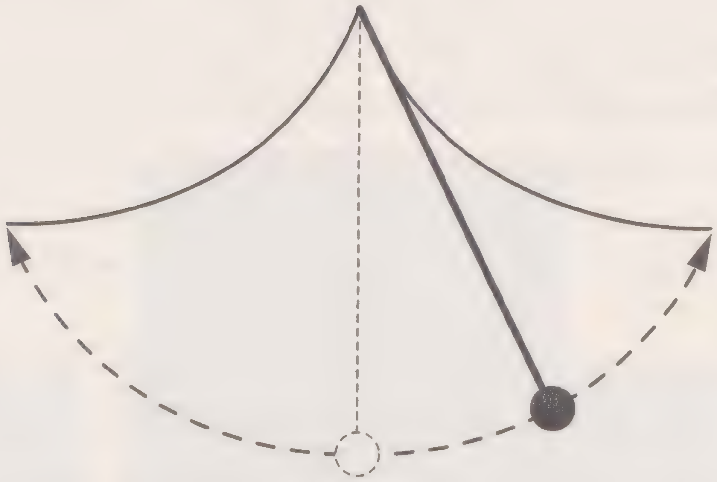
In the meantime, the problem had come to the attention of Newton. While we do not know whether he considered it an affront to his intellect, what we do know is that the day after learning of the problem, he had solved it. He sent his solution to the Royal Society and a Latin translation appeared in *Acta Eruditorum*, published anonymously because the editors did not know the author. The same issue published solutions by other authors. Perhaps somewhat annoyed, Johann read them, saw that they were correct and immediately recognised the author of the anonymous attempt. "I know the lion by his claws," he is reported to have said. Leibniz, Ehrenfried Walther von Tschirnhaus, the Marquis de l'Hôpital and Johann's brother, Jacob, also contributed solutions to what became known as 'the brachistochrone problem' – from the Greek βραχίστσ (the shortest) and χρόνσ (time). The cycloid turns out to be a brachistochrone curve, i.e. the curve that is covered in the least time by an object under the action of gravity.

The cycloid is also a tautochrone or isochrone curve, in the sense that a particle placed at random at any of its points will arrive at its lowest point in the same time.



On a cycloid, four equal movable particles dropped at different points arrive at the lowest point in the same time. The arrow indicates the acceleration of each. The x and y axes show the arc covered (s) plotted against time (t). Time is equal regardless of the length of the arc, so the end result is that when dropped simultaneously, the particles also arrive simultaneously at the lowest point of the cycloid. The cycloid is a tautochrone curve.

Huygens, is his treatise on clocks, drew on this phenomenon and invented a cycloidal pendulum.



Oscillation of a Huygens-style pendulum; Huygens was a 17th-century Dutch mathematician.

The pendulum does not describe an arc of circumference but rather a cycloid, and is isochronous. Its amplitude is unimportant because the curve described is tautochronous (or isochronous). This discovery led to the invention of more accurate pendulum clocks.

Why do honeycombs have hexagonal cells?

For bees the question may be academic, but not for geometers. And for a certain category of philosophers the question is loaded with significant unknowns: do bees act on the basis of a divinely inspired geometric instinct? What is the evolutionary purpose of having such behaviour pre-programmed into their genome? Do wax cells put pressure on each other to form hexagonal prisms? And while we're speculating, why aren't the cells square or irregular in shape?

Let's start with the principle. The term tiling is generally used to refer to any covering of a plane with pieces of equal size, whether they are regular, convex, irregular or concave in shape, and have straight or curved sides. Pappus of Alexandria (3rd-4th centuries AD), praised "the sagacity of bees" and, referring to their honeycombs, observed that of all the regular figures that could be tiled, the hexagon was the most efficient, in the sense that it offered the smallest perimeter. Therefore, if we choose to accept the teleological argument that bees will try to use the least possible wax to construct cells, then we begin to see why they choose this design. It requires the least wax.

Not all sages in the centuries that followed agreed and some, including Kepler and Darwin, preferred the theory that the pressure exerted on adjacent cells meant that the most natural shape, the circle, became distorted and formed a hexagon. Bees in fact built circular prisms, they said, but outside factors squeezed them together so they became hexagonal, and beautifully symmetrical honeycombs.

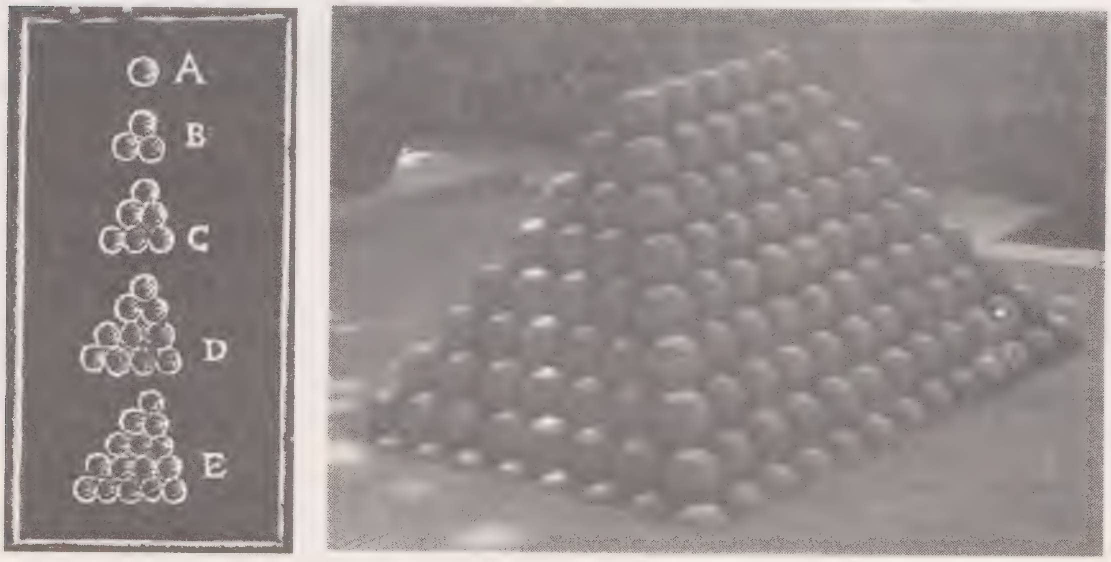
The hexagonal form of the honeycomb has been a subject for debate among geometers.

Little by little the geometers unpicked the knot of unknowns, particularly thanks to the contributions of László Fejes Tóth (1915-2005), who proved that of all regular or irregular convex polygons that tile a plane, the regular hexagon produces the smallest perimeter for a given area. After this, relatively little work remained to be done. The American Thomas Hales (b. 1958), who had already proved Kepler's sphere-packing conjecture, turned his attention to the bees problem and after a few short months produced a satisfactory solution: hexagonal tessellation is the most efficient method, more so than any non-convex shape or indeed any shape at all, including those with one curved side or more than one curved side.

The same argument holds true for floor tiles: if you want to tile a flat surface, hexagonal tiles are the best option.

Kepler and the oranges

Johannes Kepler (1571-1630) will go down in history first and foremost for formulating the astronomical laws that bear his name and not for his work as a mathematician, but we all owe him a great amount in this respect. Not only did he focus on such down-to-earth matters as barrel capacity and shape or the shape of snowflakes, he also produced two no less famous conjectures – one on bees and their honeycombs, and the orange-packing conjecture. In its most bellicose form, the latter asks what is the best and most efficient method for storing cannonballs; in its more light-hearted version, Kepler wondered how best to pile oranges. There was already an established method: since earliest antiquity oranges had been stored in uniform layers in which each fruit is tangential to another twelve, with the oranges in one layer sitting in the hollows formed by the layer below, and so on.



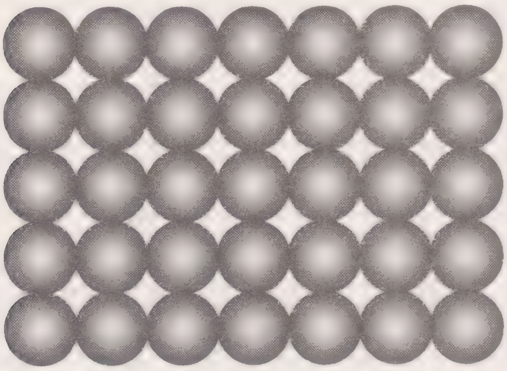
The best method for storing cannonballs was studied by Johannes Kepler, as shown by the diagram on the left, taken his work Strena Seu de Nive Sexangula, *of 1611.*

Friendly grocers, when storing their fruit, and Sir Walter Raleigh, when packing his cannonballs, were already using what geometers call face-centred cubic packing, which has an approximate density of 74% (density, according to a loose definition which is precise enough for our purposes, is the volume of oranges or cannonballs divided by total space). But, is it the best? This was not known in 1609, when Kepler made the first reference to the problem in a letter to his astronomer friend Thomas Harriot, who was in turn a friend and employee of Sir Walter Raleigh. In any case, if we draw oranges at random from a bag, and place them in any old pile, is it possible that an arbitrary configuration of oranges, perhaps a one-in-a-trillion chance, might be, by pure coincidence, the configuration with the optimum density? A complete formal proof may never be produced. Calculations carried out in 1992 showed that this approach yielded densities of the order of 0.64, far below the 0.74048 density achieved by the grocer.

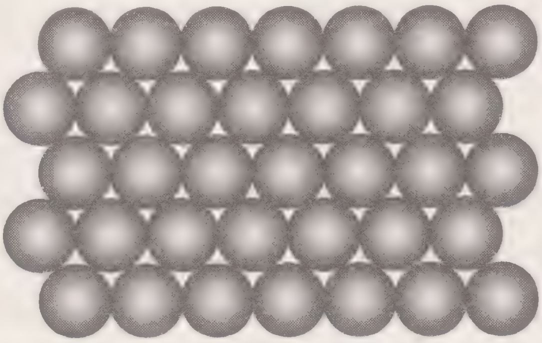
RALEIGH'S PREOCCUPATIONS

Sir Walter Raleigh (ca. 1554–1618), the famous English politician and sailor, was interested in the storage of munitions in his fleet. What concerned him was not the problem of storing spherical items which had interested Kepler – in fact, he was devoid of any mathematical interest except how to reduce the number of his enemies – but rather a very specific related question: What was the best method for arranging a square number of cannonballs in the shape of a pyramid with a square base? He just wanted an easy method of solving the problem and maximise a ship's capacity for storing arms. It is a minor arithmetical problem, which can be solved with a Diophantine equation. The solution is to arrange the balls in a slightly unstable pyramid shape, with a height of 24, and to pile up the balls in conventional layers, each sitting in the hollow formed by the other four.

If we approach the problem from a dimension function perspective, we soon see that there are only two possible networks on a two-dimensional plane.



Square packing.



Hexagonal packing.

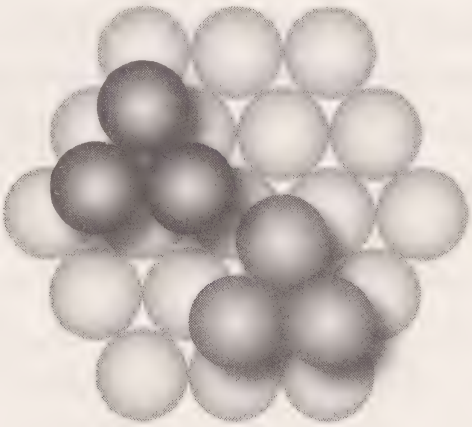
The 'networks' join the centres of the circles. The packing structure on the right gives the following density:

$$\frac{\pi\sqrt{3}}{6} \approx 0.9068996821,$$

which is the result we are looking for. If the network is raised to three dimensions, it gives cubic and hexagonal networks; the maximum density

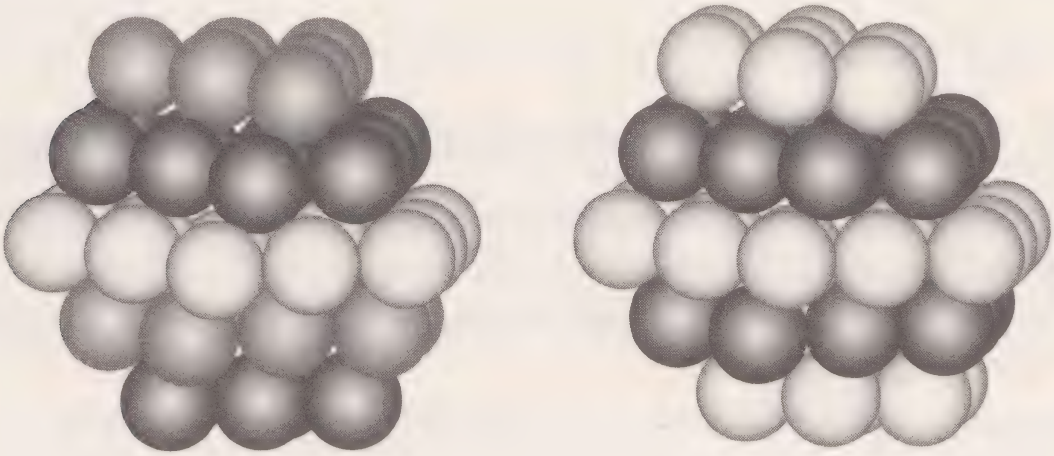
$$\frac{\pi\sqrt{2}}{6} \approx 0.74048$$

is obtained using face-centred cubic packing and hexagonal close packing. There are, essentially, two packing options:



Packing options over two layers.

Arranged over a number of layers, these two options produce, at each stage, two very similar but geometrically distinct packing structures.



The two packing options.

Both satisfy the condition that each new sphere must be placed in a hollow formed by the layer below, as in the piles of oranges. We now know that these three-dimensional sphere packing structures are optimal, but we have only known it for a few years.

Thomas Hales (b. 1958) solved this then 400-year-old conjecture in 2002. Hales used linear programming methods, optimisation theory and methods from other related fields, and not one but several computers. The complicated nature of the problems and the enormous complexity of the tests – which required a computer, as they went beyond human capabilities – made checking the result an ordeal. The referees announced that, as far as they were concerned, they were 99% certain that the proof was correct, but they could not state it with any more certainty. It seems that thanks to a new team and a more elaborate proof – and the increasing capabilities of computers – a meticulous check may finally be possible. And this brings us to a key point: to what extent are proofs that require a computer acceptable? Some – the majority – say that they are fine, and some say they aren't, and the latter category includes many first-rate professional mathematicians.

Chapter 2

A Journey Through the Euler Universe

Mathematicians have thus far tried in vain to
discover some order in the sequence of prime numbers,
and we have reason to believe that it is a mystery
that the human mind will never penetrate.
Leonhard Euler

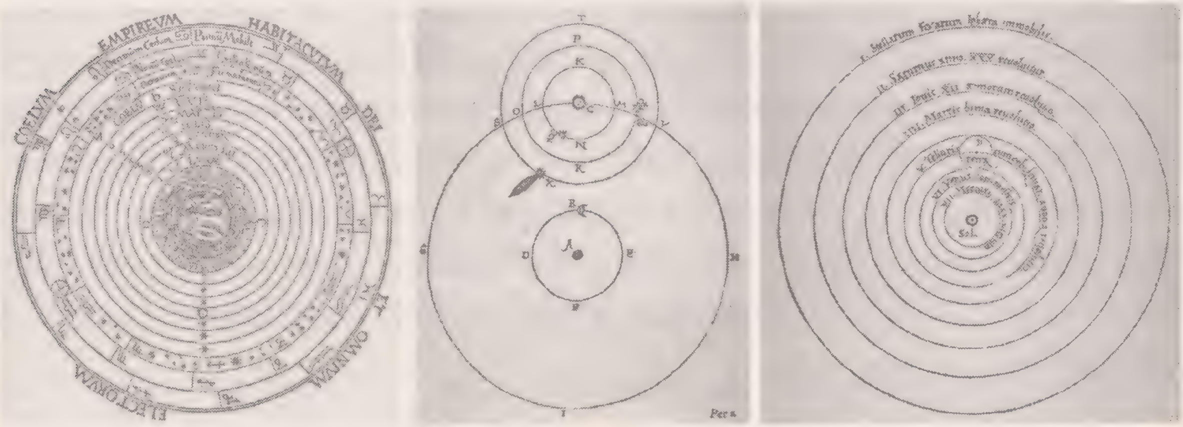
The Swiss Leonhard Euler (1707-1783) is without doubt one of the great figures in the history of mathematics. Euler (pronounced more like 'oiler') defined an era and was massively prolific. His complete works fill 76 tomes (and even then some works are missing) and all this despite the fact he suffered from problems with his eyesight almost his whole life! In addition, Euler's era saw the development of mathematical analysis, something of a sudden flourishing of reasoning and scientific practices. During this period, freedom of thought also began to spread. Dogma was still a factor but people began to question it. Euler stands out as a milestone, a beacon, a landmark of a new era.

The problem that didn't interest Sherlock Holmes

In Arthur Conan Doyle's first Sherlock Holmes story, *A Study in Scarlet*, Doctor Watson is astonished: the great detective seems unaware of heliocentrism. He doesn't know – or care – that the planets orbit the Sun.

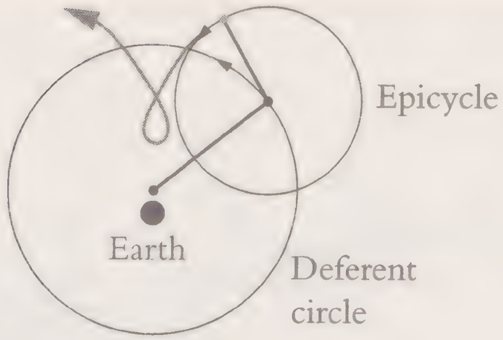
> "What the deuce is it to me? You say that we go round the Sun. If we went round the Moon it would not make a pennyworth of difference to me or to my work."

These words make sense coming out of Holmes' mouth. Let's imagine them in the mouth of a smallpox-scarred, half-crippled subject of the Holy Roman Empire in the 16th century, who has seen several of his children die, is married to a woman he doesn't love, is desperately trying to stop his elderly mother being condemned as a witch, and earns a pitiful salary that he hasn't been paid because of political complications that are completely beyond his control. We would certainly be forgiven for assuming that he would have even less reason than Sherlock Holmes to care whether the planets are orbiting or standing still. Well, we'd be wrong, because this luckless German was a mathematician, Johannes Kepler (1571-1630). It certainly was important to know which celestial body orbited which for his work. Many books and even a number of novels have been written about this figure, and it would take as many words to describe his misfortunes as his mind, which to our modern eyes may seem strange and contradictory, but clearly brilliant to anyone with the slightest scientific knowledge. It was from the works of Nicolaus Copernicus (1473-1543) that Kepler learned about the theory of heliocentrism, the belief, prohibited by the all-powerful Catholic Church, that stated that Earth and the other planets orbited the Sun. Kepler's belief in the theory never wavered.



The geocentric system (with Earth at the centre of the Universe and the stars orbiting around it), as shown in the left-hand image, was losing ground to the heliocentric system (where the Sun occupies the central position). An intermediate position was proposed in Tycho Brahe's hybrid system, combining geocentrism and heliocentrism (centre).

In the past, many theories were put forward to explain the natural world – immovable and divine, according to Aristotelianism – and the movements of the celestial sphere. We won't go so far as to suggest that it was a daily concern of the man and woman in the street, but nor was it unimportant. Observers had already noted that in their apparent paths around the Sun – their orbits – many planets seemed to retrace their steps for a certain period, and complex mechanisms had been conceived, such as the epicycles of Aristarchus of Samos (310–230 BC), to explain these phenomena.



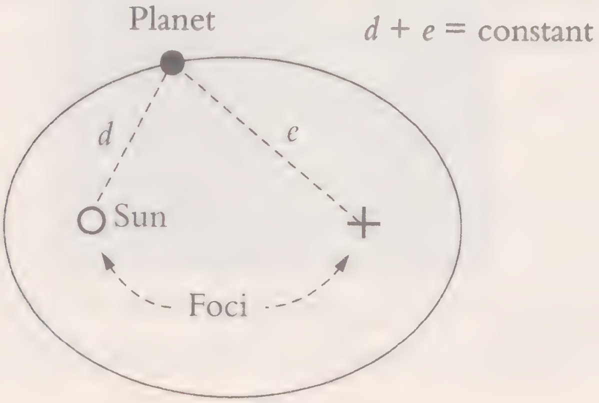
If we assume that a heavenly body moves in a circular orbit but describes another smaller circle (deferent circle) within that orbit, this results in epicycles which, viewed from the centre, suggest that the star is tracking back in its orbit.

Heliocentric theory did not rule out the possibility of epicycles and only a fully consistent theory of celestial mechanics provided a plausible explanation for them. Copernicus' theory, however, when applied correctly, did away with many imperfections at a stroke and it is no surprise that many thinkers welcomed it. Kepler certainly did.

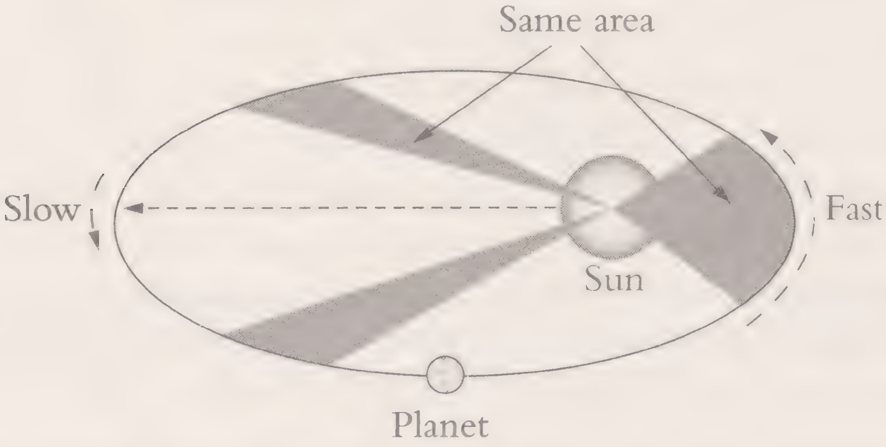
During the course of his very eventful life, one figure, Tycho Brahe (1546-1601), played a particularly central role. Tycho was a famous astronomer, the 'imperial mathematician' to Rudolf II, and a fantastic observer, a man who never made a single mistake in his measurements. He died unexpectedly, leaving Kepler to continue his astronomical work – the production of the monumental Rudolphine Tables – as they are known in the field – with details on the positions of the largest celestial bodies. Kepler based his vision of the Universe on this data.

Kepler published many books during the course of his life. But he will go down in history for his three laws, drawn up between 1609 and 1618, and stated in his work *Harmonices Mundi (The Harmony of the World)*, the most mathematically impressive of his publications. Kepler's three laws can be summarised as follows:

1. The orbits of the planets are elliptical, with the Sun at one of the two foci.



2. A line joining a planet and the Sun sweeps out equal areas during equal intervals of time.



3. The square of the orbital period of a planet is directly proportional to the cube of the semi-major axis of its orbit. This third law is incredibly important because it links the size of each orbit to the time it takes a planet to travel along it.

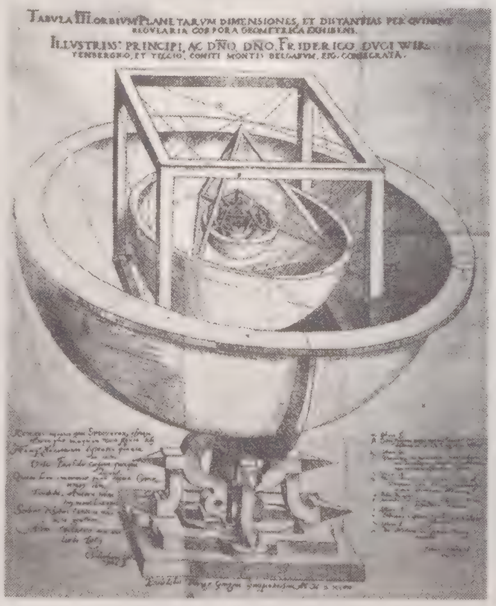
The eccentricity of the ellipse is key: if the laws merely stated that the orbits were circular, as it was conventional to assume at the time, the velocity of the planets would be constant – and what astronomers call *anomalies* would go unexplained. But Kepler discovered that the idea of circular orbits was naive, primitive and false. Kepler's three laws hold true. Combined with Copernicus' heliocentric system, they provide a response to the almost eternal question: how do the celestial bodies move?

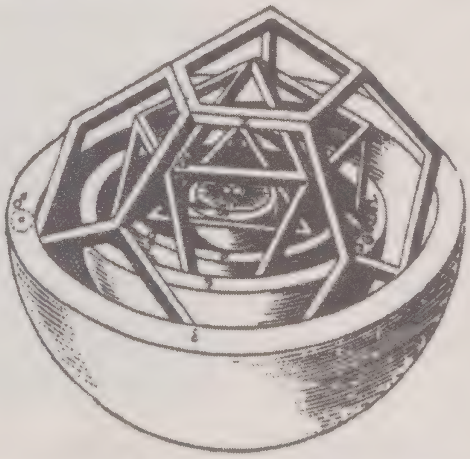
Johannes Kepler, mathematician and astronomer, is regarded as a key figure in the evolution of the scientific method.

A CONTROVERSIAL FIGURE

Among modern scientists, Kepler is a controversial figure; something of a cross between a mediaeval mystic and a modern professional scientist. He was a deeply religious man, and believed that the Holy Trinity were represented, as it is by the Father, Son and Holy Spirit, by the Sun, the celestial sphere and the interstellar void. For years he lived by horoscopes, made no clear distinction between astrology and astronomy, and gave credence to such peculiar ideas as the 'music of the spheres' and the polyhedral model of the orbits of the Solar System. But Kepler was also interested in down-to-earth matters like barrel measurements, the shape of snow crystals and, as we saw in the last chapter, the shape of honeycombs and the best method for stacking spheres.

Using spheres inscribed and circumscribed inside and outside Platonic polyhedra, Kepler tried to prove that the orbits of the planets, each one in the shape of a polyhedron, were governed by a form of geometric harmony of divine origin. Kepler was very fond of this idea, although it was soon proved to be false. The diagram on the right shows a close-up on the inner spheres, which is difficult to see in the diagram on the left.


TABVLA III ORBIVM PLANETARVM DIMENSIONES, ET DISTANTIAS PER QVINQVE REGVLARIA CORPORA GEOMETRICA EXHIBENS.
ILLVSTRISS: PRINCIPI, AC DÑO. DNO. FRIDERICO, DVCI WIRTENBERGICO, ET TECCIO, COMITI MONTIS BELGARVM, ETC. CONSECRATA.

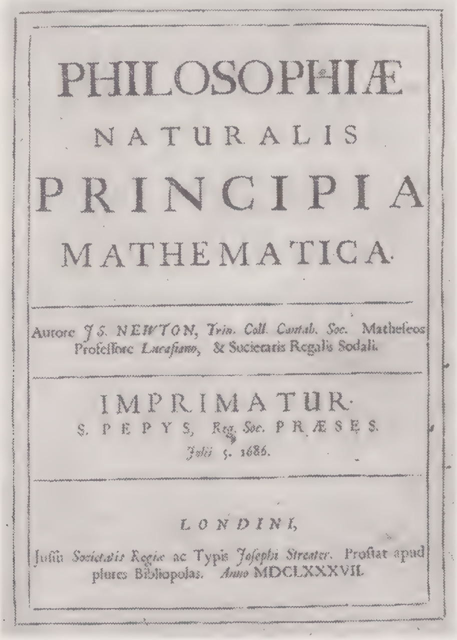


In reality, Kepler did not demonstrate anything. His observations are purely empirical, a description of reality. However, the task of deciphering them can only be undertaken using the intellect and tables of data. It can't be said that all astronomers fell at his feet to adore his three laws. The welcome was frosty to begin with, but opinion gradually turned in his favour.

Nearly one hundred years later, in his *Philosiphiae Naturalis Principia Mathematica*, Sir Isaac Newton (1643-1727), after a detailed manipulation of differential calculus, deduced Kepler's three laws from his own laws of motion. A key assumption for this deduction is the inverse-square law, which states that the attraction between two objects is inversely proportional to the square of their separation distance. One way of presenting Newton's calculation in terms of Cartesian coordinates is the following system of three differential equations:

$$m\frac{d^2x_i}{dt^2} = \frac{-kx_i}{\left(\sum_{n=1}^{3} x_n^2\right)^{\frac{3}{2}}}, \qquad i = 1, 2, 3,$$

which when solved give Kepler's laws. It could then be said that the circle had been closed. Celestial objects, whether or not they mattered to Sherlock Holmes, move in accordance with Kepler's laws and, what's more, must necessarily do so, in accordance with Newtonian mechanics.



PHILOSOPHIÆ
NATURALIS
PRINCIPIA
MATHEMATICA.

Autore *JS. NEWTON*, *Trin. Coll. Cantab. Soc.* Matheſeos
Profeſſore *Lucaſiano*, & Societatis Regalis Sodali.

IMPRIMATUR.
S. PEPYS, *Reg. Soc.* PRÆSES.
Julii 5. 1686.

LONDINI,

Juſſu *Societatis Regiæ* ac Typis *Joſephi Streater*. Proſtat apud
plures Bibliopolas. *Anno* MDCLXXXVII.

Cover page of Sir Isaac Newton's work of 1687 (translating as Mathematical Principles of Natural Philosophy), in which he states the law of universal gravitation, from which Kepler's laws are deduced.

The Basel problem

Basel, Basilea, Basle, Bâle: these are the most common western names for the beautiful Swiss city on the banks of the Rhine. Residents of Basel have included Vesalius, Jung, Erasmus, Nietzsche and Paracelsus, along with the Bernoulli family and Leonhard Euler, both of whom are associated with the problem of the sum of the reciprocals of the squares:

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\ldots=?$$

This problem occupied many of Europe's finest minds until Euler solved it with one of his juggling acts of calculus. It is hard to know what to admire more, the inventiveness or the audacity of the invention. The problem of the sum of the reciprocals of the squares was first proposed by the Italian Pietro Mengoli (1626-1686) in 1644. Gottfried Wilhelm Leibniz (1646-1716), Johann Bernoulli and his son Jacob all attacked it without success. Unlike the harmonic series

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots,$$

which is divergent, in our case the series converges and is in fact equal to

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\ldots=1.6449340668482264364724151666460251892189499012\\ 0679843773555822937000747040320087383362890061975870\ldots,$$

a figure that Euler knew but to fewer decimal places. It is thought that he knew it to six decimal places, which would probably have required him, given the slow convergence of the series, to sum around a thousand terms. It is also possible that Euler, whose numerical abilities were impressive, indeed almost inhuman, suspected that this number was $\frac{\pi^2}{6}$, the result he was looking for. What we do know is that suspecting a result is a good start when looking for a solution. Let's follow the winding path of this reasoning even though we know in advance that various steps present a number of problems and need to be refined, which happened later.

If we start with Taylor's famous series

$$\sin x=x-\frac{x^3}{3!}+\frac{x^5}{5!}-\frac{x^7}{7!}+\ldots$$

we know that it cancels itself out if x is cancelled out, in other words $\sin x = 0$ when $x = 0, \pm\pi, \pm 2\pi, \pm 3\pi\ldots$ In this way, assuming that a series will behave like a polynomial, since in reality it is a very long polynomial, application of the fundamental theorem of algebra will convert it into a product of monomials of the type $x - \alpha$, where α is a solution:

$$x-\frac{x^3}{3!}+\frac{x^5}{5!}-\frac{x^7}{7!}+\ldots=\\ =K(x)(x-\pi)(x+\pi)(x-2\pi)(x+2\pi)(x-3\pi)(x+3\pi)\ldots$$

Then K is an unknown numerical constant. Working on the right-hand side:

$$x-\frac{x^3}{3!}+\frac{x^5}{5!}-\frac{x^7}{7!}+\ldots=K(x)(x^2-\pi^2)(x^2-4\pi^2)(x^2-9\pi^2)\ldots$$

we see that every term in the form $x^2-\lambda^2\pi^2$ on the right is zero if and only if $1-\frac{x^2}{\lambda^2\pi^2}$ is zero. So let's rewrite the terms on the right in the form

$$x-\frac{x^3}{3!}+\frac{x^5}{5!}-\frac{x^7}{7!}+\ldots=K'(x)\left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{4\pi^2}\right)\left(1-\frac{x^2}{9\pi^2}\right)\ldots$$

where $K'=K(-\pi^2)(-4\pi^2)(-9\pi^2)\ldots$, and dividing by x we get:

$$\frac{\sin x}{x}=1-\frac{x^2}{3!}+\frac{x^4}{5!}-\frac{x^6}{7!}+\ldots=K'\left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{4\pi^2}\right)\left(1-\frac{x^2}{9\pi^2}\right)\ldots$$

And as $\lim\limits_{x\to 0}\frac{\sin x}{x}=1$, we can conclude that $K'=1$. So, there remains

$$1-\frac{x^2}{3!}+\frac{x^4}{5!}-\frac{x^6}{7!}+\ldots=\left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{4\pi^2}\right)\left(1-\frac{x^2}{9\pi^2}\right)\ldots,$$

which is a series equal to an infinite product. No problem, according to Euler. We methodically calculate the product and separate the (infinite) terms x^2 from the product of the right-hand side. There remains the equation

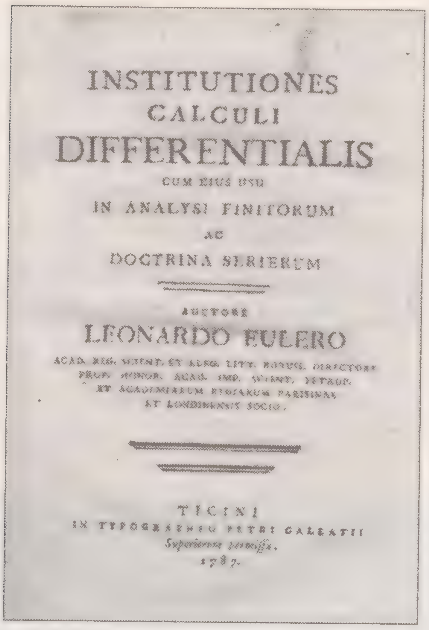
$$-\frac{x^2}{3!}=-\frac{x^2}{\pi^2}-\frac{x^2}{4\pi^2}-\frac{x^2}{9\pi^2}-\ldots$$

And dividing both sides by $-\frac{x^2}{\pi^2}$ this gives

$$\frac{\pi^2}{6}=1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\ldots,$$

which we wanted to find out.

Anyway, once Euler knew where he was heading, he retraced his steps and several years later added rigour to the demonstration, of which there still exist innumerable versions, some employing only integral calculus. In *Institutiones Calculi Differentialis* (1755) he summarised all his results.



INSTITUTIONES
CALCULI
DIFFERENTIALIS
CUM EIUS USU
IN ANALYSI FINITORUM
AC
DOCTRINA SERIERUM

AUCTORE
LEONARDO EULERO
ACAD. REG. SCIENT. ET ELEG. LITT. BORUSS. DIRECTORE
PROF. HONOR. ACAD. IMP. SCIENT. PETROP.
ET ACADEMIARUM REGIARUM PARISINAE
ET LONDINENSIS SOCIO.

TICINI
IN TYPOGRAPHEO PETRI GALEATII
Superiorum permissu.
1787.

Cover page of an edition of Foundations of Differential Calculus *published in 1787. In this text Euler published his research into the problem of the sum of the reciprocals of the squares.*

After calculating the sum of the reciprocals of the squares, Euler pursued his work on fourth powers and higher. He did not know this, but he was plunging deeper into the wild territory of the Riemann zeta function, defined by

$$\varsigma(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\ldots \qquad \Re(s)>1.$$

for complex numbers the real part of which is greater than 1.

In short, Euler proved that

$$\varsigma(2)=\frac{\pi^2}{6},\quad \varsigma(4)=\frac{\pi^4}{90},\quad \varsigma(26)=\frac{2^{24}76977927\pi^{26}}{945}.$$

This was a highly commendable result, which foreshadowed more recent results.

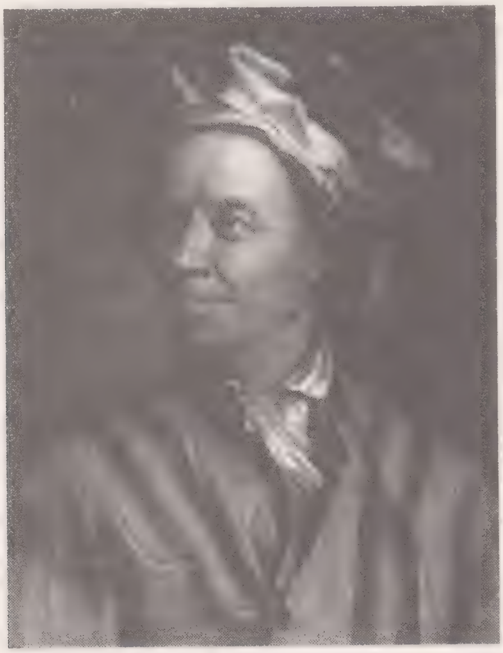
Nevertheless, we still don't know of any simple formula in the style of the previous formulae to calculate, for example, the value of $\varsigma(3)$, nor the value of the zeta function for any odd integer. In fact, the zeta function is one of the great challenges of modern mathematics. To be clear, we do know, for example, the value of $\varsigma(3)$; it is equal to:

$$\varsigma(3)=1.2020569\ldots,$$

and it is a value that even has a name – Apéry's constant, which is irrational, but we don't know whether it is transcendental. It is also possible to know the value of the zeta function at odd integers. What is unknown is not the value, but rather an analytic expression in the style of the fabulous values discovered by Euler for the first even integers. Because – you tell me – do modern formulae like the following

$$\varsigma(3)=\frac{\pi^3}{28}+\frac{16}{7}\sum_{n=1}^{\infty}\frac{1}{n^3(e^{\pi n}+1)}-\frac{2}{7}\sum_{n=1}^{\infty}\frac{1}{n^3(e^{2\pi n}+1)}$$

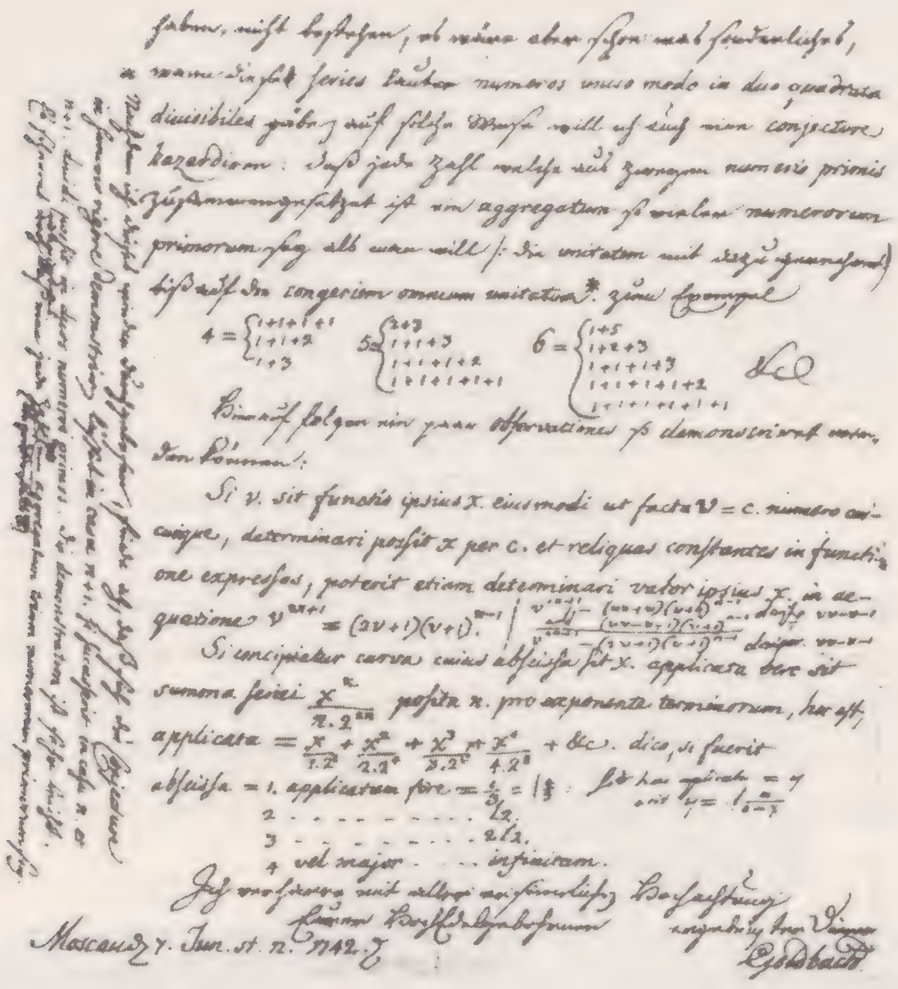
seem a little too complicated?



A portrait of Leonhard Euler in which his eye problems can be clearly seen. Euler lost the sight in one eye, and then in the other, but never let it stop him pursuing his mathematical work.

Goldbach's conjecture

In 1742, the Prussian mathematician and historian Christian Goldbach (1690–1764) gained immortality for writing a letter – a lengthy missive – to Euler. Like Euler, Goldbach was living in Russia, and it was easier for him than others to correspond with the genius. In his letter, he explained to Euler his belief that any even integer greater than 2 could be expressed as the sum of two prime numbers. In fact, the story is a little more complicated, as Goldbach regarded 1 as prime and the original draft differed slightly from our description, but you'll forgive us for not going into it in detail because it is a morass of linguistic tangles and hidden conclusions.



Page from the letter that Goldbach wrote to Euler containing the conjecture discussed in this section.

Goldbach's conjecture has all the ingredients for enduring scientific appeal. It relates to prime numbers; anyone can understand it; hundreds, perhaps thousands of brilliant minds have foundered in their attempts to solve it; and to date – as far as we know – no solution has been found. Popular novels have even been written, like Apostolos Doxiadis' *Uncle Petros and Goldbach's Conjecture*, about a fairly inconsequential subject that anyone can learn about by sharpening their pencil and jotting down the pairs of integer partitions of the number 1,000:

1,000 = 3 + 997 = 17 + 983 = 23 + 977 = 29 + 971 = 47 + 953 =
= 53 + 947 = 59 + 941 = 71 + 929 = 89 + 911 = 113 + 887 = 137 + 863 =
= 173 + 827 = 179 + 821 = 191 + 809 = 227 + 773 = 239 + 761 = 257 + 743 =
= 281 + 719 = 317 + 683 = 347 + 653 = 353 + 647 = 359 + 641 =
= 383 + 617 = 401 + 599 = 431 + 569 = 443 + 557 = 479 + 521 = 491 + 509.

At first glance, these partitions seem to confirm not only that any even integer greater than 2 can be expressed as the sum of two primes, but also that that sum can be written in many ways. When Doxiadis' novel was published, the British publishing house Faber and Faber offered, for a period of two years, a million dollars to anyone who could prove or disprove the conjecture. However, the publishers clearly knew the dice were loaded in their favour. Even this incentive changed matters.

The conjecture has been shown to hold true as far as 10^{18}, without any exception. Numerical segments through 10^{300} have also been tested. The conjecture still holds true. Or to put it another way, as Popper might say, it is never falsified.

Goldbach's so called 'weak conjecture' states that "all odd numbers greater than 7 can be expressed as the sum of three odd primes" and if Goldbach's 'strong' conjecture were solved then the weak conjecture would automatically be solved, as the weak theorem is deduced from the strong. The generalised Riemann hypothesis, one of the Clay Institute's seven Millennium Prize Problems, also involves Goldbach's weak conjecture. If the weak conjecture were solved, it would not solve the strong conjecture, but it would demonstrate that any even number could be obtained by summing four primes. From 4 to 2 is still a leap,

THE WEAK CONJECTURE

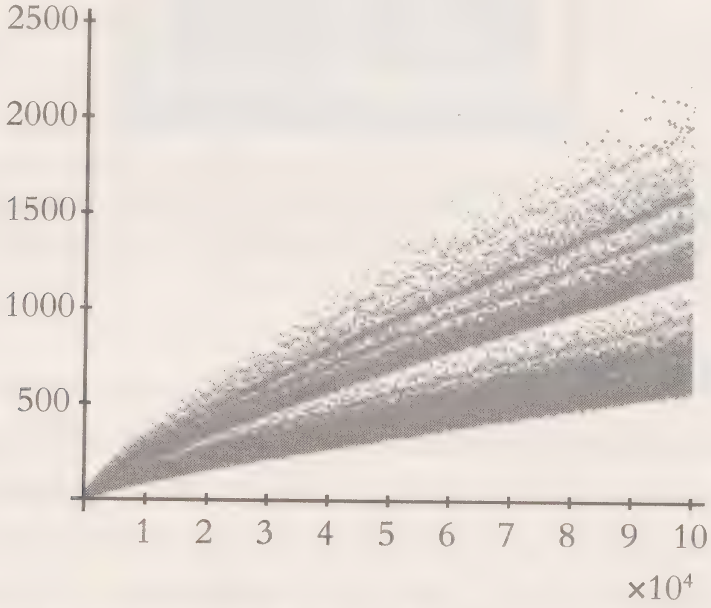
Lev Schnirelmann, one of the mathematicians who tackled Goldbach's conjecture.

Ivan Vinogradov (1891–1983) proved in 1937 that any sufficiently large odd number is the sum of three primes. Unfortunately, experts now believe that 'sufficiently large' means something in the order of $3.33 \chi 10^{43,000}$, which makes this excellent approach to the weak conjecture impractical, even for computers. Chen Jing-Run (1933–1996) demonstrated in 1973 that any sufficiently large even number was the sum of one prime and one semiprime (the product of two primes), which is an excellent result. In 1931, the Russian Lev Schnirelmann (1905–1938), a few years before he committed suicide, proved that any integer greater than 1 can be written as the sum of not more than *C* primes, where *C* is a constant. The initial value of *C* was gradually reduced (it is important to note that merely having a constant limit *C* to the number of primes is a major step forward), and Olivier Ramaré eventually got it down to seven primes in 1995.

one that might take months, or perhaps centuries. The greater weakness of the 'weak'conjecture has made it the focus of the most serious attacks, as the box on the previous page shows.

It has now been proved that the density of even numbers that do not satisfy the conjecture is zero. In other words, almost all even numbers satisfy it. But thus far nobody has managed to eliminate the 'almost' from that description.

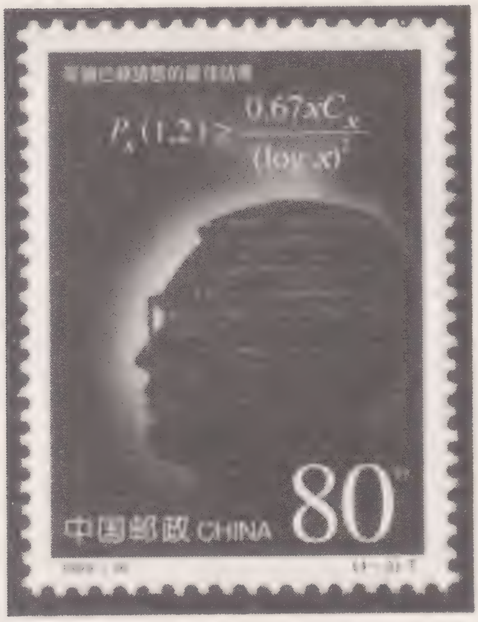
When we plot even integers on the x axis and their number of possible expressions as sums of two primes on the y axis, a characteristic image is produced in the shape of a comet tail, as you can see in the graph below.



In 2006, people began to study the fractal properties of this curve. It is worth noting that, the greater the number, the greater the number of possible sums. This rule is valid in general, but not when applied to every specific case.

To give a clearer idea of the number of possible methods, this simple table might be useful.

Number	Sums of two primes
10	2
100	6
1,000	28
10,000	127
100,000	810
1,000,000	5,402
10,000,000	38,807
100,000,000	291,400



A postage stamp issued by the Chinese government in celebration of the achievement of its citizen Chen Jing-Run in demonstrating a result that approximates Goldbach's conjecture. The words at the top of the stamp, describe it as "the greatest attempt to solve Goldbach's conjecture".

The three-body problem

Another problem that has become famous, but would be too lengthy to go into in depth and too incomprehensible to do it properly, is the three-body problem, which has nothing to do with the transmigration of the soul, or with Sherlock Holmes and the infamous Doctor Moriarty – who was an astronomer – or with sexual morals. It has to do with Newton and celestial objects. It began with two bodies – Johann Bernoulli (1667-1748) solved this problem – and has been extended to *n* bodies, but the fascination with three bodies persists. It is an old mechanical puzzle which entails, broadly speaking, finding out what happens when three physical bodies orbit around each other.

In Newton's time, people were thinking of three bodies like the Sun, the Earth and the Moon. Nowadays we might talk about an asteroid under the influence of Jupiter and the Sun; or a planet and two binary stars.

The general *n*-body problem entails solving a set of second-degree differential equations described with a vector formula like

$$m_i\ddot{a}_i = G\sum_{j\neq i}\frac{m_i m_j(a_j-a_i)}{\left\|a_j-a_i\right\|}, \qquad i=1,\dots,n,$$

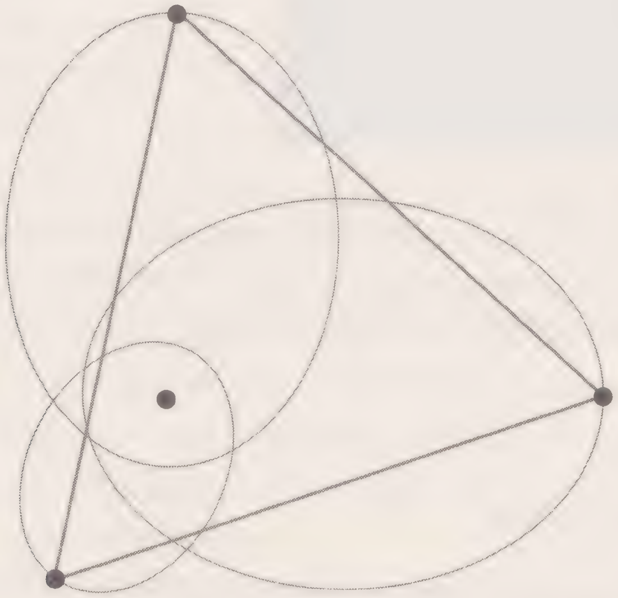
where initial values are given for the positions $a_i(0)$ with $a_i(0) \neq a_j(0)$ for all $i \neq j$, and the velocities $\dot{a}_i(0)$. The masses of each body are represented by m_k. When $n = 3$ the three-body problem arises.

In the past, specific (although sometimes very general) three-body problems have been fully and practically solved, but not the general problem. We have to use computers to get useful results.

When we discuss the three-body problem, in reality we are referring to the 'restricted', more accessible three-body problem which assumes that the orbits are coplanar and one of the bodies has a virtually negligible mass. This problem, with various variations, can be regarded as solved, but the general problem cannot.

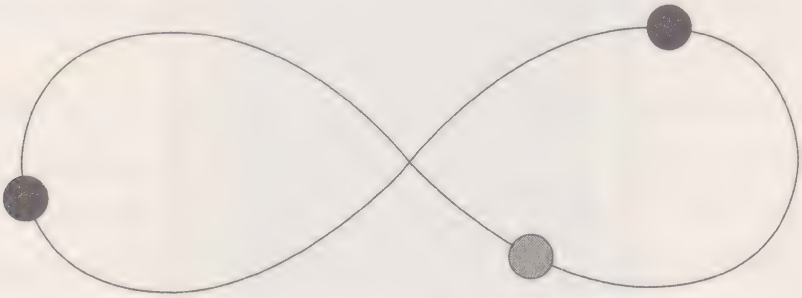
The first, famous and successful attempt to solve the restricted problem was made by Euler. Hot on his heels, although with distinct caveats, and in many cases conditions that constituted significant generalisations, followed Lagrange, Jacobi, Laplace, Adams, Le Verrier, Poincaré, Hill, Sundman, Birkhoff and many others. The restricted three-body problem (disregarding quirks, like collisions) has at least one solution discovered by Karl Frithiof Sundman (1873-1949), although his is underpinned by a numerical series that remains impractical today.

Of all the solutions found, a special place is reserved for the periodic solutions (Euler, Lagrange, Hill), and of these, Lagrange's solution stands out for its elegant language.

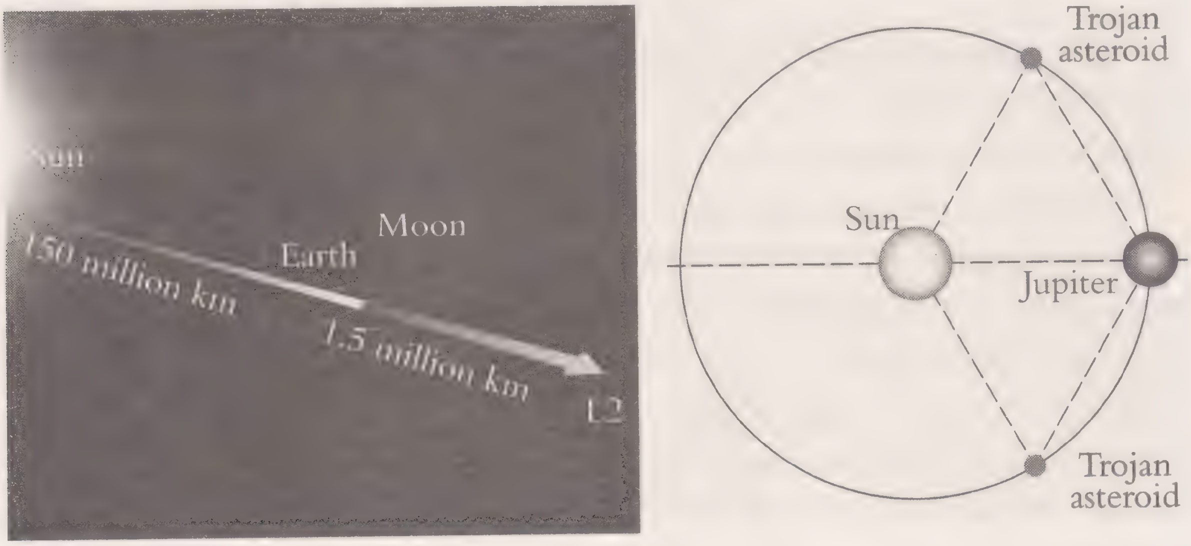


A Lagrange solution to the three-body solution;
here the masses of the orbiting objects involved are in the proportion 1: 2: 4.
The orbiting objects are placed at the vertices of an equilateral triangle.

The striking thing is that not long ago, in the late 20th century, new periodic solutions were developed – by Carles Simó (b. 1945) – in which three bodies of equal mass dance uniformly one after the other, in a figure of eight. The orbits are known, appropriately, as choreographies.



However, non-periodic approximations of the three-body problem result in a collision, or at the least chaotic, unpredictable motion.



On the left, the second Lagrangian point of stability or libration (L2) – a geostationary point that is one out of a total of five. These are part of the solution given by Lagrange to his version of the three-body problem. In proximity to Jupiter (right) the Greek and Trojan groups of asteroids also occupy Lagrangian points in relation to the Sun and Jupiter.

Legendre's conjecture

Our fascination with prime numbers has not diminished with the passing of time; indeed, our curiosity has only increased. The conjecture proposed by Adrien-Marie Legendre (1752-1833) is still unproven despite two centuries having passed since he published it in the 1808 edition of his *Theory of Numbers*.

Portrait of Adrien-Marie Legendre, author of the eponymous conjecture, painted in 1820 by Julien-Leopold Boilla as part of his series of watercolours of famous mathematicians.

The Russian mathematician and physicist Lev Landau (1908-1968) later boosted its fame by including it in his very select list of unsolved problems alongside Goldbach's conjecture, the twin prime conjecture and the near-square prime conjecture (which posits the possible infinity of primes in the form $x^2 + y^4$).

Legendre's conjecture refers to the abundance and distribution of prime numbers and states that "between two consecutive square numbers, n^2 and $(n+1)^2$, there is always at least one prime number". In fact, there seems always to be more than one.

Chen Jing-Run demonstrated in 1975 that in this gap there is always one prime or semiprime (product of two primes, which may be equal), but this statement does not solve Legendre's conjecture because one of those irritating coordinating conjunctions (the 'or') is lurking in the middle. Joseph Bertrand (1822-1900), meanwhile, conjectured (but did not prove; this was left to Chebyshev) that there is at least one prime in the gap between a number n and its double $2n$. But this excellent proof does not solve Legendre's conjecture either (although it may seem to at first glance). In 1984 the existence of one prime between $n-n^{\frac{23}{42}}$ and n was demonstrated, which improved on Bertrand's result, but did not solve Legendre's conjecture. In 2008 Shiva Kintali seemed to prove the conjecture for sufficiently large numbers, but not for all numbers.

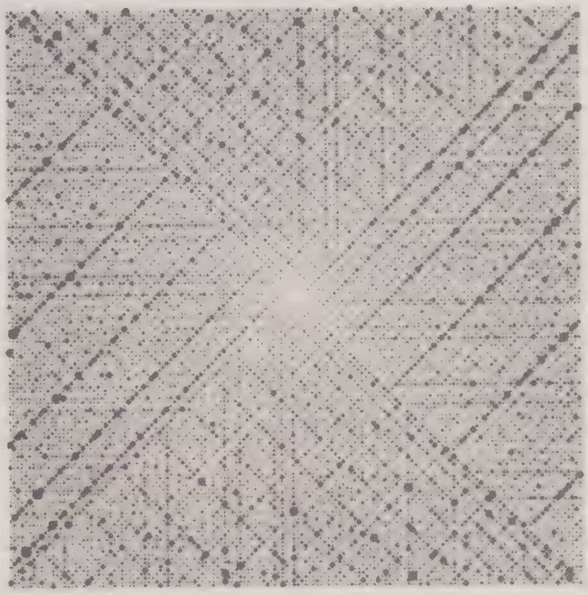
For the moment, what we can say (but it remains a conjecture) is that the gap between successive prime numbers p and $p+1$, will be of the order of $\sqrt{p}$, but only if the conjecture and Legendre's conjecture are both true. In fact, conjectures have been made that improve on this result, but they are all merely conjectures, a tangle of conjectures in the shadow of the original, which remains unsolved although a solution edges closer every day...

LEGENDRE'S CONJECTURE AND THE ULAM SPIRAL

It follows that if Legendre's conjecture is correct, the Ulam spiral, named in honour of the man who discovered it, Stanislaw Ulam (1909–1984), will give a prime number in every revolution. What does this mean?

```
37 — 36 — 35 — 34 — 33 — 32 — 31
|                             |
38   17 — 16 — 15 — 14 — 13   30
|    |                   |    |
39   18    5 —  4 —  3   12   29
|    |     |         |   |    |
40   19    6    1 —  2   11   28
|    |     |             |    |
41   20    7 —  8 —  9 — 10   27
|    |                        |
42   21 — 22 — 23 — 24 — 25 — 26
|
43 — 44 — 45 — 46 — 47 — 48 — 49 ...
```

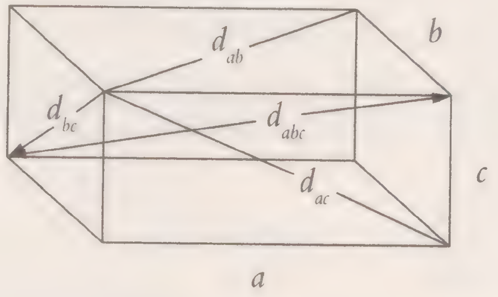
This is an Ulam spiral, which can be easily constructed by laying out the natural numbers in a spiral. When a sufficiently extensive spiral is displayed, mysterious lines of high prime number density appear, many without any explanation. Legendre's conjecture spices up the matter even further.



Expansion of an Ulam spiral showing lines with high densities of prime numbers.

An elusive brick

An Euler brick is a particular type of straight parallelepiped. Consider the following straight parallelepiped, also called a cuboid in geometry.



Straight parallelepiped.

If it has the edges a, b and c, and the face diagonals:

$$d_{ab} = \sqrt{a^2 + b^2}$$
$$d_{bc} = \sqrt{b^2 + c^2}$$
$$d_{ac} = \sqrt{a^2 + c^2}$$

and all are representable by integers, then it is what is known as an Euler brick. When the space diagonal is also an integer (the four space diagonals are equal):

$$d_{abc} = \sqrt{a^2 + b^2 + c^2},$$

the shape is called a perfect cuboid. Note that the same result is obtained in the field of rational numbers, and it is the consequence of something as simple as Pythagoras' theorem. If the denominators of the irreducible fraction of the numbers d_{ab}, d_{bc}, d_{ac} and d_{abc}, were α_{ab}, α_{bc}, α_{ac} and α_{abc}, the 'rational' brick would become an integer brick if its edges were multiplied by the LCM $(\alpha_{ab}, \alpha_{bc}, \alpha_{ac}, \alpha_{abc})$.

No examples of perfect cuboids have been found, although Euler bricks have, and as time passes and research continues, it seem increasingly clear that the perfect cuboid does not exist.

Equations where solutions can only be integers are called Diophantine equations. Therefore, finding a perfect cuboid rather than an Euler brick entails nothing less than finding the solution to the system of Diophantine equations:

$$x^2 + y^2 = z^2$$
$$x^2 + v^2 = w^2$$
$$y^2 + v^2 = t^2$$
$$y^2 + w^2 = s^2$$

A parametrisation of the above conditions (while it does not provide all the solutions) is

$$(a,b,c) = (|u(4v^2 - w^2|, |v(4u^2 - w^2|, |4uvw|)$$

with

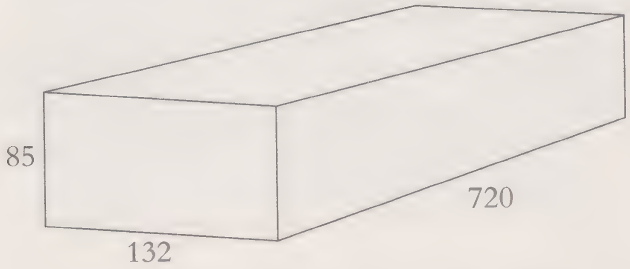
$$a^2 + b^2 + c^2 = f(t,s)(s^2 + t^2)^2$$
$$u = 2dt$$
$$v = v^2 - t^2$$
$$w = s^2 + t^2$$
$$f(t,s) = s^8 + 68s^6 t^2 - 122s^4t^4 + 68s^2 t^2 + t^8$$

but none of these solutions gives edges for perfect cuboids, nor can they give them, as was demonstrated in 1972.

Euler bricks do exist, and the following are examples of measurements of their edges.

44-117-240
85-132-720
88-234-480
132-351-720
140-480-693
160-231-792
176-468-960
240-252-275
480-504-550
720-756-825

The first set of measurements, which are the smallest of all, were discovered in 1731 by Paul Halcke, an accountant.



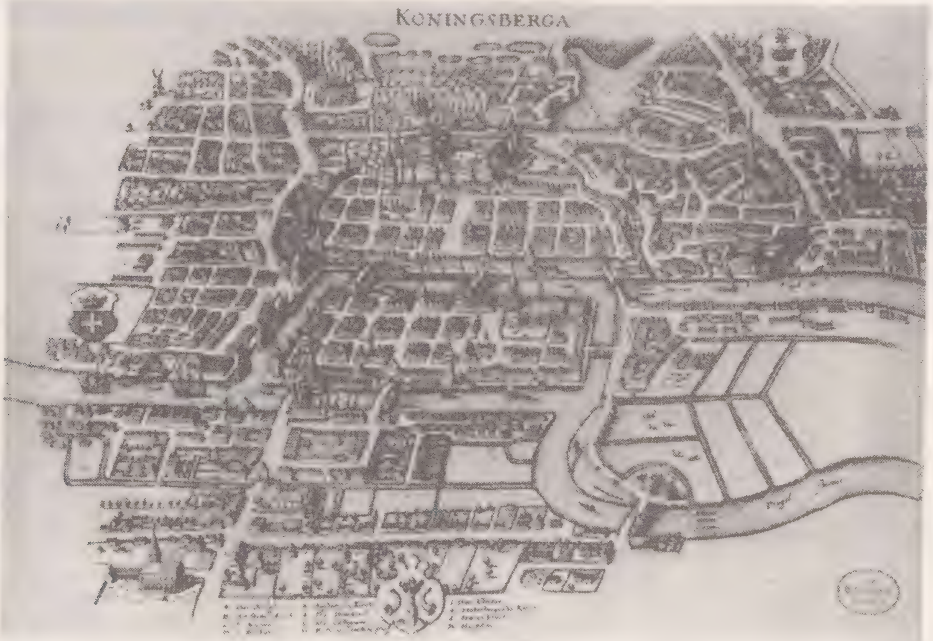
Measurements of the edges of an Euler brick.

In 2009 perfect parallelepipeds were shown to exist, although unfortunately they are not cuboids because their faces, while parallel, are not perpendicular to each other. This somewhat weaker conjecture was made by the mathematician Richard Guy (b. 1916), a visionary with a fertile imagination who discovered the amazing unstable body with only 19 faces, the *gömböc.*

The first computer-based search yielded 27 perfect parallelepipeds. Using computers, unsuccessful attempts have been made to discover Euler bricks with edges of the order 10^9. We have nothing to show for them. Fortunately, we don't build walls using Euler bricks.

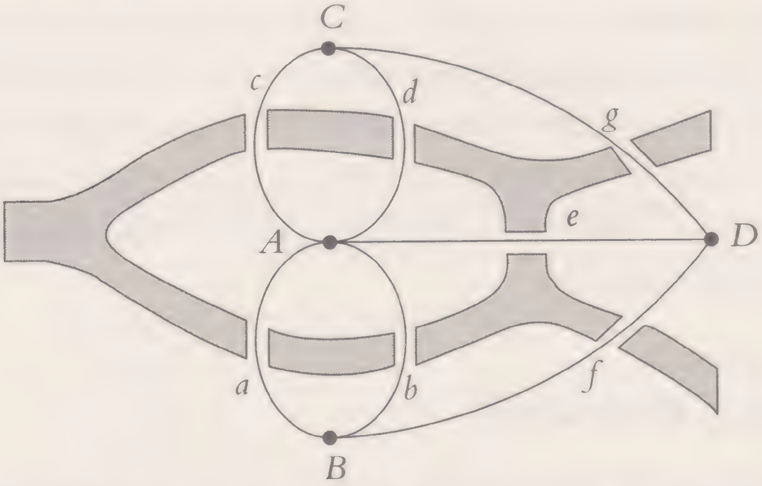
The bridges of Königsberg

Euler used the bridges of Königsberg to create a new science. In the mathematician's time, the city belonged to Prussia – it is now the Russian city of Kaliningrad, which lies on the Baltic coast between Poland and Lithuania, a short distance from Gdansk (formerly Danzig). It is set on the Pregel River and, in Euler's era, specifically in the 1730s, seven bridges connected the city's two large islands to the mainland and each other. Nowadays, alas, such a scenario cannot be reproduced because the city's layout has changed and some of the bridges are no more. What Euler was presented with was a city laid out as in the following engraving.



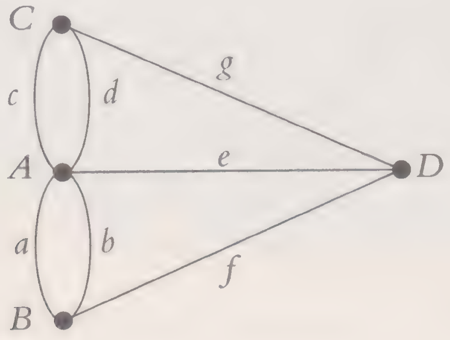
Map of the city of Königsberg from the mid-17th century.

The following graphic shows the elements relevant to the problem set by Euler: the two river islands (designated *A* and *D*), the seven bridges over the river (with lower case letters), and the two areas of mainland (designated *B* and *C*).



The problem Euler set for walkers in the city was what we would now call a brainteaser: could you find a route through the city that crossed each and every bridge only once, and crossed them completely every time? After analysing the problem, in 1735 Euler announced a solution: there was no such route and walkers hoping to check for themselves on the ground would end up wandering endlessly between the bridges.

Euler's demonstration is now available in many sources and the original in Latin can be found in *Solutio problematis ad geometriam situs pertinentes* (*The Solution of a Problem Relating to the Geometry of Position*), although it is not relevant to us here. Euler realised that the crucial aspect of the problem was the bridges and the potential routes that they enabled. More specifically, Euler reduced the problem to one of nodes (areas of the route, represented using points) and edges (in this case the bridges, which in the diagram are links between nodes), eliminating distances and the shapes of routes, and basing his analysis purely on schematic ideas.



Euler based his reasoning on four nodes connected by seven edges; note that the pathways are now points or vertices and the 'bridge crossings' are represented by lines. Without making it explicit, he decided to think in terms of topology, the branch of modern mathematics in which we disregard distances and shapes and focus only on what really matters. Euler is now considered to have invented graph theory, an application of combinatorial topology, which is in turn a branch of topology.

The solution he found is ingenious and is based on the following reasoning:

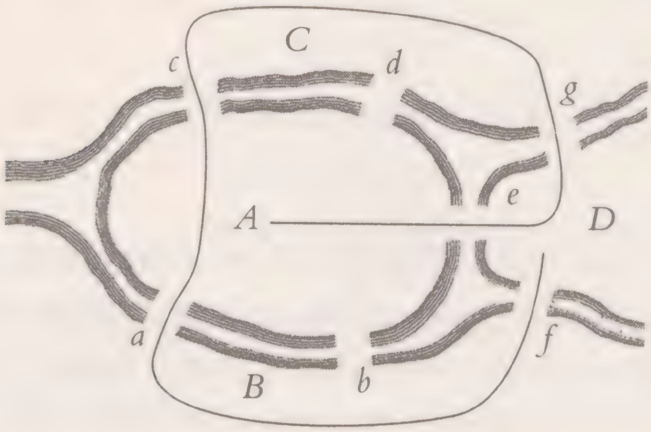
- If an edge enters a node that is not an endpoint, another edge must leave that node.
- There must therefore be an even number of edges entering and leaving each node.
- All the nodes in the Königsberg system have an odd number of edges.

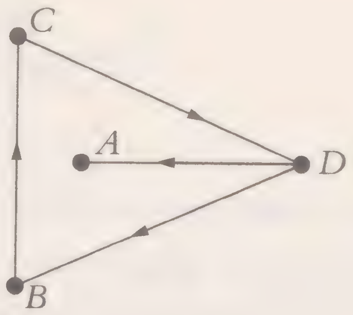
However, we will not follow every step of Euler's laborious intellectual journey, as it is long and takes time and attention. Anyone interested can turn to a specialist book or website for details; the important thing to note is that the demonstration is elementary, yet not at all simple!

What Euler demonstrated in his reasoning amounts to stating, in short:

> The bridges can be crossed exactly once if, with the exception of at most two, all the nodes have an even degree.

At the beginning of this section we noted that modern Kaliningrad is not like old Königsberg; in fact, two of the old bridges were destroyed in bombing raids during World War II, a third has been redesigned. Two short bridges were converted into one long bridge, as the following diagrams show.





The route we would be following is different now, but if we began our walk at *D* we would end up necessarily at *A* and vice versa. In a twist of fate, the route would still not be correct, strictly speaking, because it would start on one island and finish on the other. To complete it correctly, we would need to go back over the bridges to return to the departure point on the mainland. It seems that even the bombs have conspired with graph theory to make life difficult for walkers.

A 19-year-old genius

Carl Friedrich Gauss (1777–1855) was a well-known figure in his own lifetime and his contemporaries called him *princeps mathematicorum*, the Prince of Mathematicians. He was a child prodigy and, as an adult, still had phenomenal powers of mental arithmetic and memory, and an exceptional intellect to boot. All of this made him the subject of numerous anecdotes, many of which may well have been apocryphal. However, it is no exaggeration, but rather a verified historical fact, to say that he solved a classic problem – the construction of the regular polygons – when he was still a 19-year-old who had not yet decided between pursuing a career in languages or in mathematics. He is said to have opted for mathematics after this early success.

The ancient Greeks already knew how to construct – in the Greek style, using only ruler and compass – various polygons, including those with 3, 4, 5, 6, 8, 10 and 15 sides. Euclid demonstrated several constructions in his *Elements* and those that derive from the well-known constructions, where the number of sides is multiplied by 2^n (just repeatedly bisecting the central angles), are redundant. In the modern era, because of their beautiful appearance and usefulness in perspective, regular polygons have been used and reused (the pentagon in particular, because of its usefulness in ballistics, and as a basis for designing fortresses).

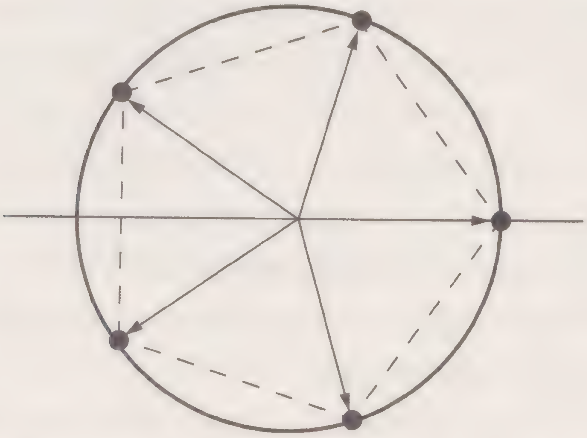
It's not that it was conceptually difficult to calculate the edge l_n of an n-sided regular polygon, as the equation

$$\frac{l_n}{2} = r\sin\frac{2\pi}{\frac{n}{2}} \text{ (which is equivalent to } l_n = 2r\sin\frac{\pi}{n}\text{)}$$

is not complicated and enables us to work with trigonometric functions like sine (unknown to the Greeks). Nonetheless, something that is conceptually simple to understand may be difficult to approach mathematically. The construction of regular polygons began to interest mathematicians again, and Gauss in particular was equal to the challenge. How could it be that someone with Euclid's reasoning abilities could not cope with a simple heptagon?

Gauss identified the construction of an n-sided regular polygon with the construction on the complex plane of solutions to the cyclotomic polynomial equation $x^n - 1$.

$$x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1 = 0$$



Constructing an n-sided regular polygon is equivalent to finding all the complex roots of the cyclotomic polynomial $x^n - 1$. In the diagram, $n = 5$, which gives the regular pentagon. Note that $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \ldots + x + 1)$.

To fully understand Gauss's solution, we first need to define Fermat numbers. A number F_p is known as a Fermat number when it is of the form

$$F_p = 2^{2^p} + 1.$$

Fermat numbers can be prime or composite. If we draw up a list like the following:

$$\begin{aligned}
F_0 &= 2^{2^0} + 1 = 3 \\
F_1 &= 2^{2^1} + 1 = 5 \\
F_2 &= 2^{2^2} + 1 = 17 \\
F_3 &= 2^{2^3} + 1 = 257 \\
F_4 &= 2^{2^4} + 1 = 65{,}537 \\
F_5 &= 2^{2^5} + 1 = 4{,}294{,}967{,}297 = 641 \cdot 6{,}700{,}417
\end{aligned}$$

we see that the first numbers are prime, but the last is not, as Euler remarked. In fact, factorising F_5, using a pencil and paper, is a commendable achievement in itself. The next example, $F_6 = 274{,}177 \cdot 67{,}280{,}421{,}310{,}721$, was factorised in 1880 by the Parisian Fortuné Landry, who dedicated much of his life to the enterprise. The probability of factorising this number is lower than playing the lottery all your life and winning the top prize, but requires slightly more intellectual effort.

It is not known whether there are any higher Fermat primes, but none has been found. Experts have not given up hope of finding them, and think that if they do exist, they will be finite numbers.

Gauss proved the following theorem: a regular n-sided polygon can be constructed with ruler and compass if and only if n is the product of 2^k multiplied by one or any number of distinct Fermat primes. In more symbolic language, if and only if it is of the form

$$n = 2^k p_1 p_2 \cdot \ldots \cdot p_m \text{ with } k \geq 0,$$

where p_i is either a Fermat prime or distinct Fermat primes.

The theorem means that regular polygons with n sides where $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 24\ldots$ are constructible.

In particular, the 17-sided polygon is derived from the following expression, discovered by Gauss:

$$16\cos\frac{2\pi}{17} = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}\,.$$

This construction required a lot of work from his contemporary Johannes Erchinger. The next Fermat numbers are the basis for genuinely enormous polygons with 257 and 65,537 sides.

The 'official' portrait of Gauss. As a figure and scientist he spanned a whole era of mathematics, astronomy and physics, as he is regarded as the co-inventor of the telegraph. The base of his tomb, in Göttingen, is a 17-sided polygon, in tribute to his first geometric discovery.

THE 257 AND 65,537-SIDED POLYGONS

In 1832 Friedrich Julius Richelot (1808–1875) gave the world the first instruction manual for constructing a 257-sided polygon using ruler and compass. His article has a title almost as long as there are sides in the polygon: *De resolutione algebraica aequationis* $x^{257} = 1$*, sive de divisione circuli per bisectionem anguli septies repetitam in partes 257 inter se aequales commentatio coronata.*

Johann Gustav Hermes (1846–1912), meanwhile, spent ten years constructing, using ruler and compass, a 65,537-sided regular polygon, a Herculean task he completed in 1894. In the end, he submitted his 200-page manuscript – but didn't publish it – to the University of Göttingen, where you can view it if you're interested, although there's plenty of information available online. What is certainly true is that some people, like John Conway, still don't believe in the demonstration, an unequivocal sign that they have started to read it. The polygon that Hermes tried to construct has so many sides it looks at first glance like a circle. The cosine $\cos\frac{\pi}{65{,}537}$ is an algebraic number, but it would take an equation of degree 32,768 to find a polynomial that has it as a root.

In search of the lost equation

The beginning of the search for solutions to second-degree equations is lost in the mists of time. The Egyptians, Babylonians and Greeks were already familiar with them and explicit references were made to them by figures like Diophantus (ca. 200/234–ca. 284/298). Nowadays, our basic textbooks include the formula that gives the roots of the equation $ax^2 + bx + c = 0$:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

which in some cases are complex conjugates, admittedly, but that is another story. Another story for another day concerns the so-called fundamental theorem of algebra, which states that any polynomial with complex coefficients of degree n has n complex solutions (a statement demonstrated by Jean-Robert Argand in 1806).

The search for the equation resumed after the Renaissance. The story, which is as convoluted as the plot of a bad detective novel, can be traced back to Scipione del Ferro (1465–1526), a mathematician who unravelled the mysteries of a special type of third-degree equation of the form $x^3 + bx = c$. One of the three solutions is obtained using the following formula:

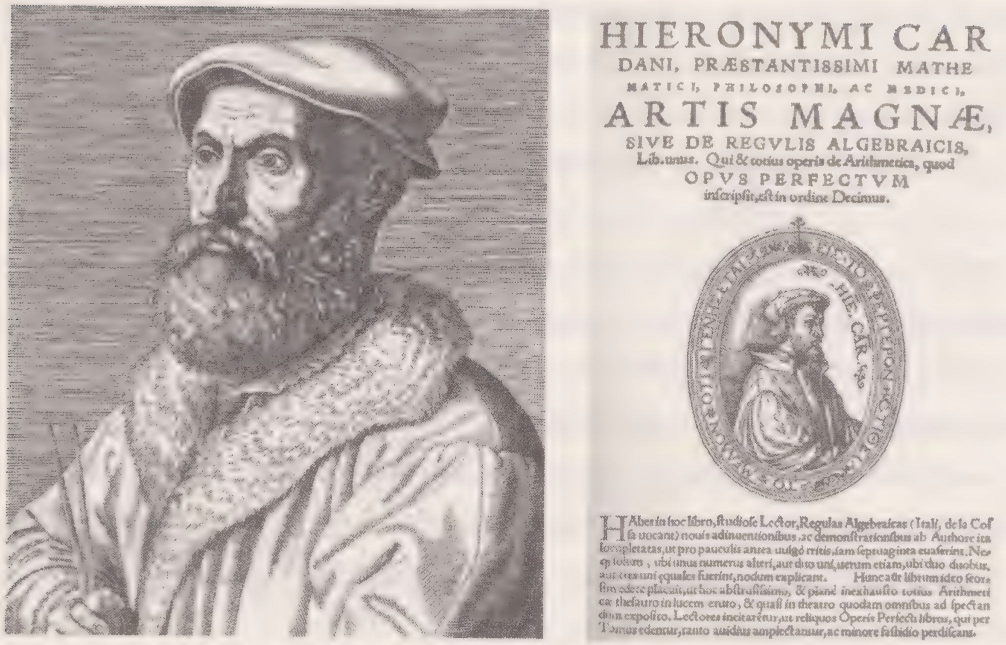
$$x = \sqrt[3]{-\frac{c}{2} + \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}} + \sqrt[3]{-\frac{c}{2} - \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}},$$

which gives us an early indicator that this subject is not straightforward.

Del Ferro took the secret to solving the equation with him to the grave, although as we will soon see, the story is a little more complicated than that. In the meantime, a mathematician was born in Brescia called Niccolò Fontana (1500–1557), who his countrymen and posterity would know as Tartaglia, because of his stammer. Tartaglia was an excellent mathematician despite his poverty, and was always looking for an academic position so that he could live more comfortably. At that time mathematical challenges were very fashionable because they brought intellectual superiority and, along with it, the best jobs, including academic and government jobs. In this case Antonio Maria Fior, Del Ferro's right-hand man and possessor of the secret formula for the third-degree equation, challenged Tartaglia, convinced that his formula would see him come out on top. But he didn't count on the genius of Tartaglia, who several days after Fior's challenge restated Del Ferro's method and enhanced it with his own personal contribution. Tartaglia ruthlessly defeated Fior and kept possession of his own method for solving third-degree equations. Two could play at that game!

Tartaglia's nemesis was Girolamo Cardano (1501–1576), the illegitimate son of a lawyer, who took an interest in various fields: he was a doctor, gambler (chess, card games, dice), cryptographer and astrologer, and like Tartaglia was always trying to carve his own niche. Cardano was desperate to know Tartaglia's method and tried everything he could including flattery; after numerous failed attempts, he tried a mix of intrigue and promises of promotion, a ploy that finally delivered him the longed-for formula, but on the condition that he reveal it to nobody. It seems Cardano reluctantly kept his word, and for a time everything was quiet, with the exception of Cardano hiring a very intelligent young assistant, Lodovico Ferrari (1522-1565). Together they had interminable arguments about Tartaglia's methods.

One day, Cardano visited Del Ferro's son-in-law and was handed the manuscript showing the solution found by the dead mathematician. Cardano now felt justified in breaking his word. After all, Tartaglia was not the only person in on a secret that Del Ferro had also known (albeit partially, remember).



HIERONYMI CARDANI, PRÆSTANTISSIMI MATHEMATICI, PHILOSOPHI, AC MEDICI,
ARTIS MAGNÆ,
SIVE DE REGVLIS ALGEBRAICIS,
Lib. unus. Qui & totius operis de Arithmetica, quod
OPVS PERFECTVM
inſcripſit, eſt in ordine Decimus.

HAbes in hoc libro, ſtudioſe Lector, Regulas Algebraicas (Itali, de la Coſſa uocant) nouis adinuentionibus, ac demonſtrationibus ab Authore ita locupletatas, ut pro pauculis antea uulgò tritis, iam ſeptuaginta euaſerint. Neq; ſolum, ubi unus numerus alteri, aut duo uni, uerum etiam, ubi duo duobus, aut tres uni æquales fuerint, nodum explicant. Hunc aũt librum ideo ſeorſim edere placuit, ut hoc abſtruſiſſimo, & planè inexhauſto totius Arithmeticæ theſauro in lucem eruto, & quaſi in theatro quodam omnibus ad ſpectandum expoſito, Lectores incitarẽtur, ut reliquos Operis Perfecti libros, qui per Tomos edentur, tanto auidius amplectantur, ac minore faſtidio perdiſcant.

Portait of Tartaglia and cover page of Ars Magna, *the book in which Cardano published the research into third and fourth-order equations.*

On top of all this, the prodigious Ferrari had discovered a method of transforming a quartic equation – a fourth-degree equation – into a third-degree equation, which is why Cardano enjoys something only just short of immortality: he knew how to solve third- and fourth-degree equations! He published his discoveries in a book entitled *Ars Magna* (1545) and made his name.

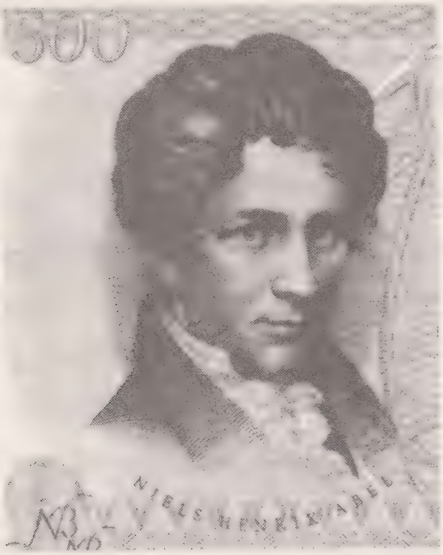
Tartaglia was furious. In his view Cardano had quite simply broken his promise. He pursued him relentlessly, and challenged him, this time with a sword in his hand and not a pen. He was so insistent that Ferrari suggested another challenge, this time mathematical. Tartaglia felt impelled to accept and Ferrari, young, prepared and ambitious, won hands down. He later died having been poisoned by his sister, so perhaps he wasn't as smart as he seemed.

After quartic equations, quintic equations proved impossible to solve. Lagrange discovered a marvellous method for solving many equations. It entailed using another equation, known as an auxiliary or characteristic equation, to help solve it by reducing the degree of the equation. Once the solutions to the characteristic equation had been found, they could be reconstructed to find the solutions to the original equation. It was an ingenious method but couldn't be applied to quintic equations. The characteristic equation was of a degree higher than 5. Something was wrong, and because something had been wrong for so many years Lagrange feared the worst – was it that fifth-degree equations were unsolvable?

Some fifth-degree equations are perfectly solvable, but the aim was not to solve simple, isolated examples but to find a formula that would work in all cases.

In 1824, the young and ill-fated Norwegian mathematician Niels Abel (1802–1829) claimed the honour of solving the fifth-degree equation problem. Paolo Ruffini (1765–1822) had already got close, but his supposed proof had a number of flaws. Abel demonstrated that there is no magic algebraic formula (sums, products, powers and their reciprocals, remainders, divisions and roots) which can solve any equation of a degree higher than five.

Abel's demonstration is impeccable, advanced and non-reproducible, and if we were to criticise it for anything – what a criticism! – it is that it merely solves the problem. It's strange, but in this case it is almost as important to solve the problem as to establish why the problem is a problem. It's also worth noting that Abel's demonstration went unnoticed in his own time. It would be some time before it gained its due recognition.



The portrait of Niels Abel has appeared on various stamps and bank notes. Since 2002, his name has also graced the prize awarded by the Norwegian Academy to make up for the lack of a Nobel Prize for mathematics.

This latter question is now answered by the Galois theory, which we won't go into in detail here because it would take a lot of space and is quite advanced. But we will try to outline it, although the explanation is somewhat vague and nebulous. Let's see. For every equation, there is a linked set of permutations of the roots that characterise the equation. This set of permutations forms a group, a relatively simple, well-studied and modern algebraic structure. For each equation, this group is called the Galois group.

An algebraic property shared by the groups is their resolvability. Galois proved that an equation was solvable with a general formula that used roots if and only if its Galois group was solvable. And as it happens, for equations of degree five and above their Galois groups may not be solvable. Then there are unsolvable equations. And this time we do know why a problem cannot be solved.

Évariste Galois (1811–1832) was a French revolutionary and mathematician who died at the age of 21 in a duel and spent the hours leading up to his death annotating his mathematical discoveries for Gauss and Jacobi (1804–1851) to read. All Galois's writings were lost for many years, but his papers were finally unearthed by Joseph Liouville (1809–1882) and published in 1846 in the *Journal des mathématiques pures et appliquées*. Liouville's work was a little overshadowed by Galois'. But this is nothing to be ashamed of, as Galois' theory is one of the great works of the human mind.

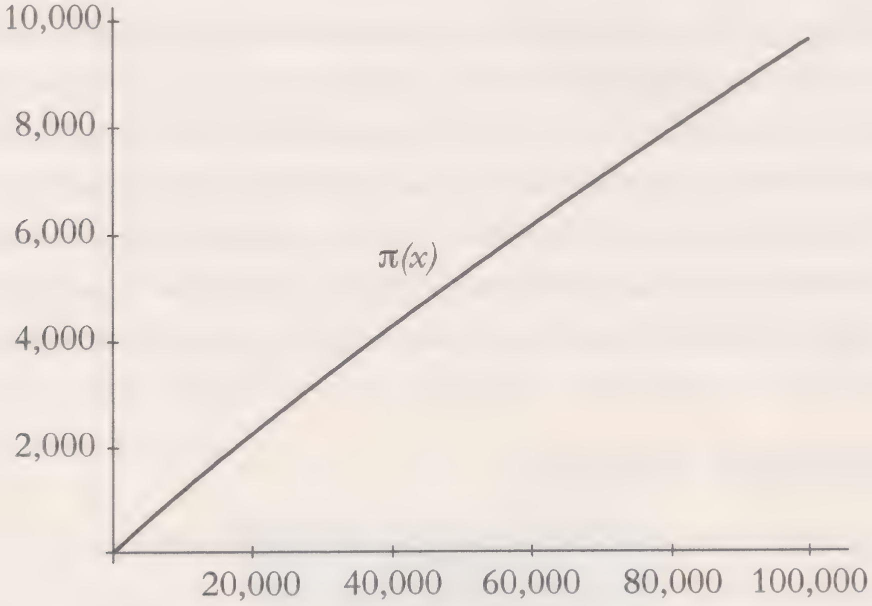
The prime number theorem

How many positive integers greater than zero that are multiples of 10 are there below a specified number n? How are they distributed? The answer is simple, because the law of the formation of these multiples is well known. They are dotted like milestones along the number sequence, separated by uniform gaps of 10. Given an n, all we have to do is go back to find the nearest multiple of 10 – subtract the last digit – and take off the zero; the remaining number is, obviously, the number of multiples of 10 lower than n that we're looking for. But if instead of multiples of 10, we choose, for example, the category of factorial numbers,

$$k! = k \cdot (k-1) \cdot (k-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$$

things begin to get a little more difficult.

What can we say now if we think in terms of prime numbers? They are definable numbers, but we do not know in principle when n is prime or not. It's very difficult to locate the nearest prime p to n, and we don't know what gap there will be between one prime p and the next. There are enormous primes separated by only two spaces (twin primes), such as the colossal pair $65{,}516{,}468{,}355 \cdot 2^{333333} \pm 1$, but also very large numerical sequences without a single prime. For example, from $(n+1)! + 2$ to $(n+1)! + n + 1$ there are n non-prime numbers, all composites. Choosing a very large n delivers numerical sequences that stretch on and on, and are prime-free. Does that sound unlikely? Take $n = 24$, for example. If you calculate it (it's difficult) you'll see that it's true. But that doesn't mean that we don't know how to tackle the question of the distribution of prime numbers. It's just that it's not an easy problem. Let's start by defining our terms. We'll call $\pi(x)$ the number of primes lower than or equal to x. Their graph when x is large looks good, as you can see below.



The table of values, as far as we currently know, is as follows:

x	π(x)
10	4
100	25
1,000	168
10,000	1,229
100,000	9,592
1,000,000	78,498
10,000,000	664,579
100,000,000	5,761,455
1,000,000,000	50,847,534
10,000,000,000	455,052,511
100,000,000,000	4,118,054,813
1,000,000,000,000	37,607,912,018
10,000,000,000,000	346,065,536,839
100,000,000,000,000	3,204,941,750,802
1,000,000,000,000,000	29,844,570,422,669
10,000,000,000,000,000	279,238,341,033,925
100,000,000,000,000,000	2,623,557,157,654,233
1,000,000,000,000,000,000	24,739,954,287,740,860
10,000,000,000,000,000,000	234,057,667,276,344,607
100,000,000,000,000,000,000	2,220,819,602,560,918,840
1,000,000,000,000,000,000,000	21,127,269,486,018,731,928
10,000,000,000,000,000,000,000	201,467,286,689,315,906,290
100,000,000,000,000,000,000,000	1,925,320,391,606,803,968,923

Prime number theorem, which sheds light on the distribution of primes, states that

$$\pi(x) \sim \frac{x}{\log x},$$

where *log x* is the Napierian (or natural) logarithm of x. The symbol ~ is read 'asymptotically equal' and means that the limit of the quotient of the two variables when $x \to \infty$ is 1, but be careful: that does not mean that the difference between the two variables tends towards zero:

$$\pi(x) - \frac{x}{\log x} \to 0,$$

since both terms may differ, for example, by a constant. Just think of the variables n and $n + 1{,}000$. It's true that they are asymptotically equal, but their difference does not tend towards zero. In fact, it is constant and equal to 1,000:

$$\frac{n}{n+1000} \to 1, \text{ but } (n+1000) - n \to 1000$$

It's clear to see that, in fact, the expression $\pi(x) \sim \frac{x}{\log x}$, is the same as writing in its place $\pi(x) \sim \frac{x}{\log (x-k)}$, where k is a constant.

We say that because the first person to propose the prime number theorem was Legendre, and he used $k = 1.08366$ because it could be deduced from his tables. We now know that the best approximation is obtained with $k = 1$, simply because we have access to better tables.

The following data present a very satisfactory approximation.

x	$\pi(x)$	$x/\log x$	$x/\log (x-1)$
1,000	168	145	169
10,000	1,229	1,086	1,218
100,000	9,592	8,686	9,512
1,000,000	78,498	72,382	78,030
10,000,000	664,579	620,420	661,459
100,000,000	5,761,455	5,428,681	5,740,304

When Gauss attacked the problem, he swapped the formulation for another, in essence equivalent to the original, but providing more refined estimations:

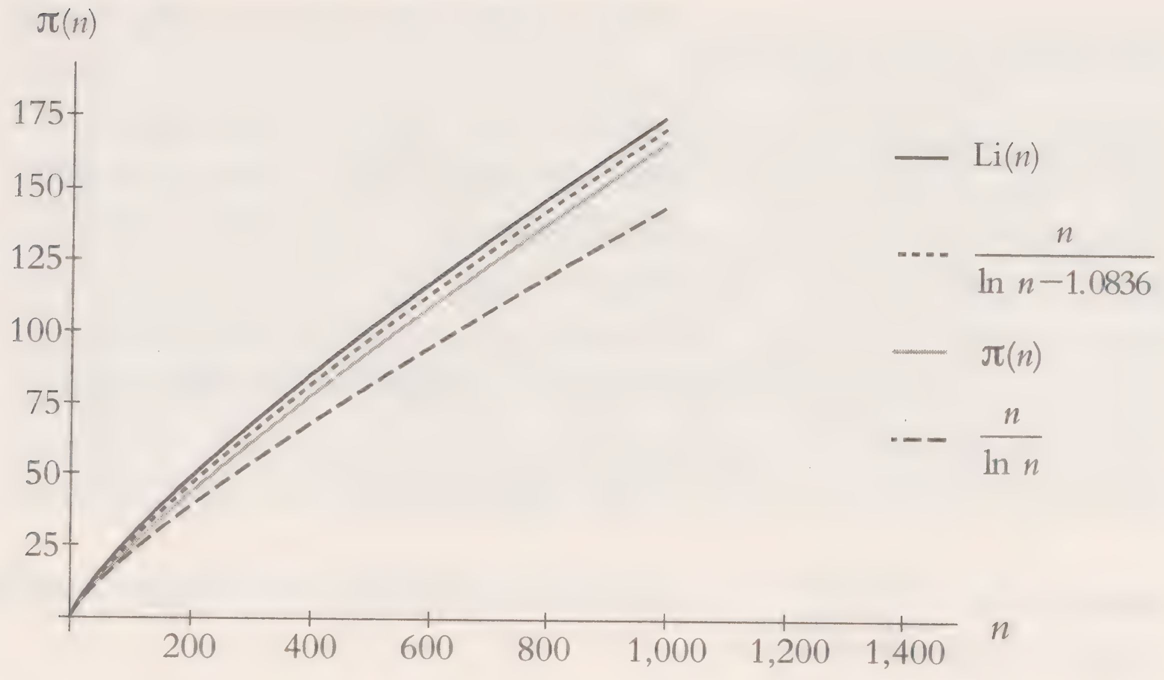
$$\pi(x) \approx Li(x) = \int_2^x \frac{dt}{\log t}$$

The new function introduced here is *Li(x)*, called the logarithmic integral function. Gauss, who often filed his discoveries away in a drawer without publishing them, noted this in 1843 in a letter to his astronomer colleague and friend Johann Encke (1791–1865), but he did not reveal it. Gauss's idea, with its logarithmic integral function, is splendidly ingenious, but lacks a small detail. He did not demonstrate it mathematically. He suspected it and wrote it down, but there is no record of his proving it. The proof of the theorem did not arrive until 1896 when a Belgian mathematician, Charles Jean de la Vallée Poussin (1866–1962) and another Frenchman, Jacques Hadamard (1865–1963), proved it in the same year, completely independently of each other. Both used the most advanced methods of complex analysis and the Riemann zeta function.

Charles de la Vallée Poussin (left) and Jacques Hadamard demonstrated the prime number theorem in 1896.

As demonstrated as early as 1901, the approximation error of the Gauss formula is of the order of $\sqrt{x \log x}$, in which case the famous Riemann hypothesis is verified. Yet, although more than a century has passed, the long-awaited hypothesis is still indemonstrable, to the desperation of mathematicians... and journalists, who would like to be able to break the news.

The following curves give a graphic idea of how close together the various approximations of the prime number distribution are.



To finish, a curiosity purely for non-specialists; in the graph, the $\text{Li}(n)$ curve is always higher than $\pi(n)$. The first value of n at which this no longer held true (assuming the Riemann hypothesis to be true) was designated the Skewes' number and is equal to

$$e^{e^{e^{79}}}$$

which for many years held the title of the highest number to feature in any mathematical formula. It was calculated in 1933 and is much larger than the number of atoms in the known Universe.

And the journey does not end there

We could go on for page after page, as the list of problems seems never-ending. But we will only mention a few more, such as Waring's first problem, proposed by Edward Waring (1734-1798) and solved by David Hilbert in 1909. The problem arose when someone noticed that any number is the sum of at most four cubes; and at most nine quarter powers; and (now things are getting more difficult) at most 19 fifth powers. And having got this far, can any number be said to be the sum of one fixed number of powers of order n? That is the conjecture posed by Waring and solved by Hilbert.

We might also mention the problem of the number 0.57721566490... which looks like any other ordinary number. It is produced when at the end n of the

WARING'S SECOND PROBLEM

Waring's so-called second problem asked whether all odd integers were either prime or the sum of three primes. Ivan Vinogradov (1891–1983) proved in 1937 that any sufficiently large odd number, prime or otherwise, was the sum of three primes. So what's the problem? It lies in the meaning of the words 'sufficiently large', since even an optimistic calculation gives an upper limit that is an inconceivable number, making checking it infeasible even armed with a supercomputer. Vinogradov's result amounts to magnificent progress, but does not entirely solve the problem, although it 'almost' solves it.

harmonic series $1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots$ we deduct the Napierian natural logarithm of *n* and get an ever smaller number:

$$1-\log 1=1-0=1$$

$$1+\frac{1}{2}-\log 2=1.5-0.6931471\ldots=0.8068528\ldots$$

$$1+\frac{1}{2}+\frac{1}{3}-\log 3=1.8333333\ldots-1.0986123\ldots=0.734721\ldots$$

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}-\log 4=2.083333\ldots-1.3862944\ldots=0.6970389\ldots$$

This difference stabilises and, ultimately, gives a constant amount often referred to as γ

$$\gamma=\lim_{n\to\infty}\left[\sum_{k=l}^{n}\frac{1}{k}-\log n\right]=0.57721566\ldots$$

It is called the Euler-Mascheroni constant in honour of the famous Euler and of the similarly illustrious geometer Lorenzo Mascheroni (1750-1800). Euler revealed γ in 1734 and Mascheroni went on to calculate it, correctly working it out to 19 decimal places. In case it is of any use to anybody, here are the first 150 decimal places:

0.57721566490153286060651209008240243104215933593992359880576
72348848677267776646709369470632917467495146314472498070824 8
0960504014486542836224173997644923 53…

In 2007, computers exceeded 2,000,000,000 digits.

The constant γ is important as it turns up in many unexpected places: in statistics, quantum physics, mathematical analysis and number theory. It also appears in the study of the mysterious Riemann ζ function.

We know almost nothing about γ and by this we mean that we don't know whether it is an algebraic or transcendental number; nor do we know if γ is rational or irrational. Conway and Guy have claimed that γ is transcendental. What we do know is that if it is a rational number, its period must be enormous, at no fewer than 242,080 digits.

And let's finish with a worrying and surprising equation:

$$\gamma = \sum_{n=2}^{\infty} \frac{(-1)^n \zeta(n)}{n},$$

What is the zeta function doing here? What mystery is concealed here?

Chapter 3

Mathematics Comes of Age

Why are things as they are and not otherwise?
Johannes Kepler

After a period of consolidation dominated by Euler, mathematics entered the respectable territory of the sciences that are 'difficult' by definition. It was still possible – although increasingly rare – for a single mind to get a grip on the whole field, and the problems that arose as it progressed were becoming less and less understandable to the layperson. Rare pearls of problems lingered from the past, such as Fermat's conjecture, but the new problems that were proposed could seldom be understood by the man or woman in the street, although the four-colour conjecture is an exception. Logic might demand that we deal with each problem in the chronological order in which it arises. However, some of them, like Fermat's conjecture (or last theorem), date from the 17th century but were only proven in the late 20th century, in what we would call 'our time'; that is why it is included here.

Other conjectures or problems, like those that have come out of the maturing of statistics, are mathematically very interesting but are so complex that explaining their basic precepts would inevitably take several pages; there is no sound reason for including them in a popular mathematics book. For example, a much-quoted problem goes as follows: what is the probability that the Sun will rise in the morning? Leaving aside the fact this problem and others like it have yet to be resolved, including them might make us wiser but would shed little light on the progress of mathematics. It forms part of another galaxy of interests shared with other sciences.

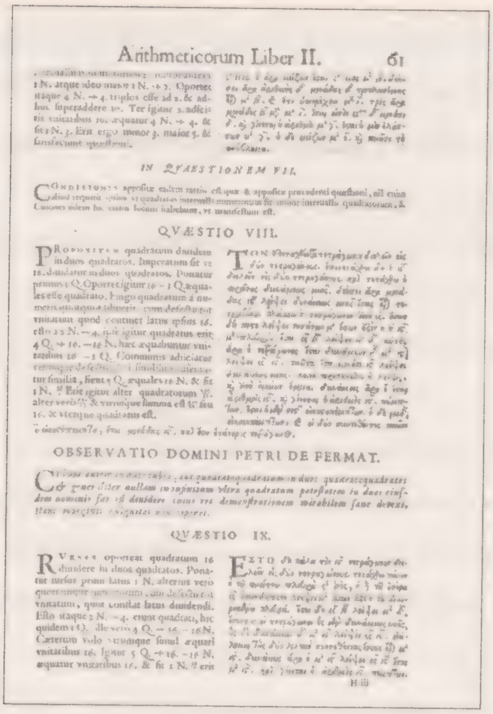
The most famous conjecture

In 1993, for the first time in history, a mathematical event made the front pages of the newspapers. Andrew Wiles (b. 1953 and later Sir Andrew) announced that he had solved Fermat's conjecture and, finally, made it a theorem. It turns out that there are indeed no three positive integers, x, y and z, that can satisfy the equation

In 1637, Pierre de Fermat (left) proposed a conjecture that would not be proved until the 1990s by the British mathematician Andrew Wiles (photograph copyright: C.J. Mozzochi, Princeton, N.J.).

$x^n + y^n = z^n$ for $n > 2$. As this was the last of Fermat's conjectures remaining to be proved, it became widely known as 'Fermat's last theorem'. This marked the end of a 356-year hunt that began with a mysterious statement by Fermat and formally ended with a conference in a Cambridge classroom.

The conjecture by Pierre de Fermat (ca. 1601–1665) – who was not in the habit of writing down his proofs – had all the ingredients needed for the plot of a bestselling book. On the one hand, it was a short and accessible statement: nothing more than the algebra we learn in school is needed to come to terms with it. In fact, a mind as keen as Hilbert had dismissed it, regarding it as a somewhat vulgar conjecture whose resolution would not amount to a major, qualitative mathematical breakthrough. However, the years passed and nobody managed to prove a conjecture that belongs to the field of number theory, a discipline regarded as quintessentially 'mathematical'. Prizes, including cash prizes, were offered to the person who could solve the problem, which began to acquire its own mythology. Indeed, in the 19th century the intellectual challenge of the conjecture persuaded the great German Paul Wolfskehl (1856–1906) not to commit suicide. He also offered a 100,000-mark prize to anyone who could solve it. Last, but not least, Fermat's own words handwritten in a book by Bachet de Méziriac in 1637 ("I've found a remarkable proof of this fact, but there is not enough space in the margin to write it") suggested the existence of a phantom proof, a kind of hidden treasure. The story of the theorem was beginning to resemble the plots of books like *Treasure Island* by Robert Stevenson and *The Purloined Letter* by Edgar Allan Poe. Fermat's conjecture has turned up in numerous places – in episodes of *Star Trek* and *The Simpsons*, in the science fiction of Arthur



Arithmeticorum Liber II. 61

IN QVAESTIONEM VII.

QVÆSTIO VIII.

OBSERVATIO DOMINI PETRI DE FERMAT.

QVÆSTIO IX.

In 1670, Fermat's son published a translation by Bachet de Méziriac (1581-1638) of a treatise by Diophantus with his father's comments in the margin. And so "Fermat's last theorem" was born.

C. Clarke and Frederik Pohl, and even in bestselling crime fiction like *The Girl Who Played With Fire* by Stieg Larsson. Yet the whole story had to be put on hold. Shortly after the solution to Fermat's conjecture was announced, threatening storm clouds began to gather on the scientific horizon. The experts had found a hole in Wiles' proof, a subtle yet significant gap. Wiles and his assistant Richard Taylor (b. 1962) took nearly two years to overcome the obstacle, but published a new and satisfactory proof in 1995. And the story doesn't end there. While working on the new proof, Wiles turned 40, the age limit for receiving the Fields Medal (the top maths award at the time), and the theorem and Wiles himself were no longer in the running for this most prestigious prize. At the 1998 Berlin congress the leaders of the International Mathematical Union were unable to award him the Fields Medal, but created a new prize, a silver plaque.

It is also worth highlighting that Fermat's successors believe they've found the mistake he made, without having access to his supposed proof! It seems that in one logical step, on what is a virtually compulsory route to a proof, a polynomial has to be decomposed into a product of prime polynomials. But something that holds true in elementary numerical or polynomial operations (every positive integer has a unique prime factorisation) is not necessarily true in the field of quadratic integers, although it may seem obvious. In the specific field of polynomials, factorisation ceases to be unique, whereas Fermat (and some of his successors) probably assumed that it was always unique. In fact, overcoming this difficulty led to the definition of so-called 'ideal numbers' and a breakthrough in modern algebra credited to Ernst Kummer (1810–1893) and Richard Dedekind (1831–1916).

Which brings us to the conjecture. We won't consider the case $n = 2$, because in this eventuality we are reduced to finding the groups of x, y *and* z that satisfy

$$x^2 + y^2 = z^2.$$

These groups of three, referred to as Pythagorean triples, are solutions to an elementary and well-known Diophantine equation and are expressed parametrically, for any positive integers a and b, such as

$$\begin{aligned} x &= a^2 - b^2 \\ y &= 2ab \\ x &= a^2 + b^2. \end{aligned}$$

Nevertheless, from that point there was no way of finding any solution; for $n > 2$ the route always seemed to be blocked. The lack of solutions for $n = 3$ was proven (Euler and possibly Fermat), for $n = 4$ (Fermat himself), for $n = 5$ (Dirichlet and Legendre), as it was for many other values. It was proven for thousands and thousands of values; in fact, it was proven for infinite values, since if the conjecture is proved for a prime number k, it automatically follows for all multiples of k. The names of Gabriel Lamé (1795–1870), Sophie Germain (1776–1831) and the aforementioned Ernst Kummer must not be forgotten. The conjecture was proven up to the prime values $n \leq 4{,}000{,}000$, but not for *any* value of n. And history teaches us to be cautious; Euler predicted, for example, that values of x, y, z and v did not exist such that

$$x^4 + y^4 + z^4 = v^4,$$

a result that nobody doubted, since Fermat's very similar statement for $n = 4$ seemed to corroborate it, until in 1988 Noam Elkies (b. 1966) proved that

$$2{,}682{,}440^4 + 15{,}365{,}639^4 + 18{,}796{,}760^4 = 20{,}615{,}673^4,$$

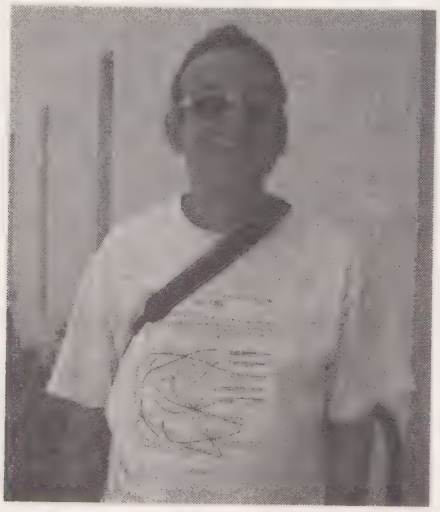
and the disappointment was almost palpable.

In 1954 Goro Shimura (b. 1930) and Yutaka Taniyama (1927-1958) found a link between elliptic curves and modular forms, two apparently very distinct and unrelated algebraic objects. An elliptic curve is a cubic equation of the following type:

$$y^2 = (x + a)(x + b)(x + c),$$

where a, b and c are non-negative integers. A modular form is an analytic equation in the field of complex numbers which, in a nutshell, exhibits a huge number of symmetries and is invariant for an order-two group of unitary matrices. Both entities are linked by a mysterious L-function in the form of a series of powers that somehow codify its deepest algebraic structures.

What the world was not expecting was that Ken Ribet (b. 1947) would prove in 1986 that if the Taniyama-Shimura conjecture were true, then Fermat's conjecture would follow. In fact, it also followed that only part of the Taniyama-Shimura conjecture was needed: a special class of curves sufficed. The incredibly difficult Taniyama-Shimura conjecture was proved in 1999 by a team of mathematicians led by Christophe Breuil, but we are already getting ahead of ourselves.

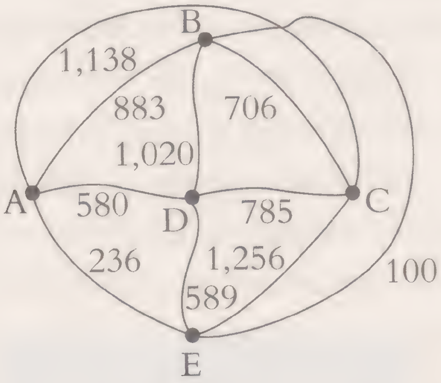


Ken Ribet, Professor at the University of California, Berkeley, established a link between the Taniyama-Shimura conjecture and Fermat's last theorem.

Wiles, an expert in the field, a brilliant mathematician and iron-willed man on a mission, shut himself away for years to think and devote all his brain power to solving the problem. In 1993, he presented his first solution, which was shown to have a flaw. In 1995, two articles published in the *Annals of Mathematics* brought the shutters down on the conjecture for good, proving it definitively. Fermat's conjecture is dead, long live Fermat's theorem!

The death of a travelling salesman

The worst that can happen to a travelling salesman is not that Arthur Miller writes a play about your life and misadventures, but rather that you are promoted; at least that's the joke in mathematical circles. Let's suppose that a salesman is tasked with visiting *n* towns by car. If he tries to do it using his common sense his calling sequence will follow some basic rules. For example, he will ensure that his route is Hamiltonian, in other words he will not call at the same town twice and he will use as little fuel as possible, i.e. he will travel the shortest possible distance. And all of the above can be expressed with an undirected graph with edges denoting the distances between vertices.



But if we want to decide which path is the best, all we can do is use trial and error and add up the distances. We just need to sketch out $\frac{4!}{2}$ routes and do twelve sums. The lowest total, which we have shown in the imaginary graph above, gives the best route. It may not seem like an act of cruelty, but if we were to promote the salesman, we wouldn't be doing him any favours. If he has to supervise, say, 50 towns, he will have to check some $5 \cdot 10^{62}$ sums before deciding. Just 20 towns would surely push him to the brink – he'd have 121,645,100,408,832,000 sums waiting for him. For *n* towns there are $\frac{(n-1)!}{2}$, sums where ! means:

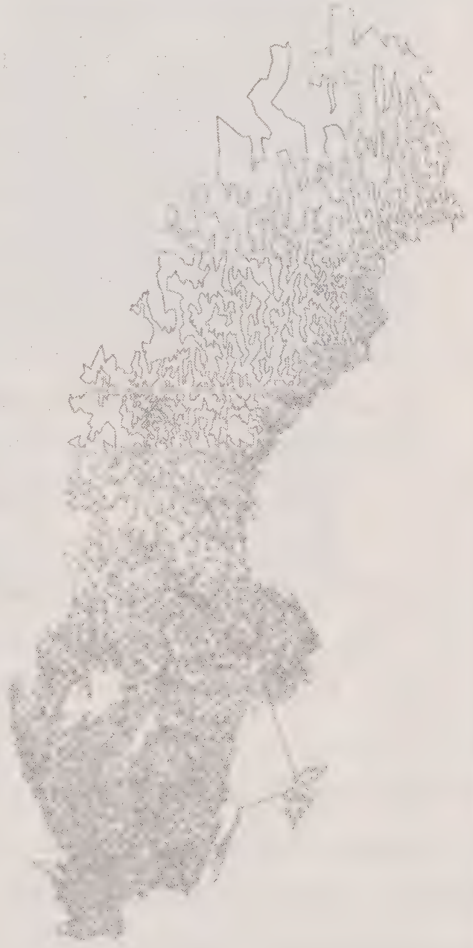
$$n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (n-1) \cdot n,$$

which denotes the 'factorial of *n*' and has the perverse habit of growing exponentially as *n* grows.

This is the travelling salesman problem, proposed somewhat loosely in the 19th century and more clearly in 1930 by various professionals, including Karl Menger (1902–1985). Its repercussions on other fields, such as the sequencing of DNA, have made it an ongoing area of interest.

PENDING A UNIVERSAL ALGORITHM...

Many heuristic and approximation approaches – including imitating the behaviour of an ant colony – to the travelling salesman problem have been devised, and in some cases extremely large problems have been solved. One example is the solution developed in 2004 by David Applegate. He and his team solved the problem for 24,978 towns in Sweden, connected in the most efficient way by a graph that involves a tour of 72,500 km. This solution no longer holds the title of 'travelling salesman problem solved for the highest number of towns', but at the time it represented a landmark. However, no universal algorithm has yet been devised that can tackle the problem in a reasonable space of time. Perhaps there isn't one, but that can be proved...



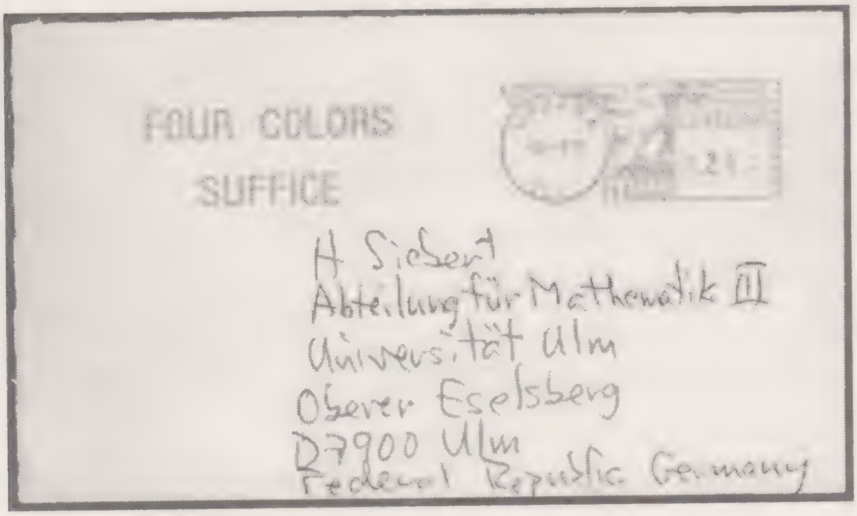
One of the shortest tours connecting thousands of Swedish towns suggested by the TSP (Travelling Salesman Problem) website developed by David Applegate.

We can disclose now that the problem has yet to be resolved, although there is a magnificent algorithm for solving individual cases, as you can see in the box. It performs a phenomenal number of sums and selects the lowest total. However, it is not a practical technique, not even with the help of computers. Algorithms exist that perform the calculations in a time of around $n^2 2^n$, which obviously grows exponentially as n increases; in the P versus NP controversy, which we will discuss later when we focus on the Millennium Prize Problems, the travelling salesman problem is classed as a *hard* problem, i.e. one of great computational complexity.

Four colours suffice

That is what the postmark said one day in 1977 when it appeared on a series of letters sent from Urbana (Illinois), a city home to an elite faculty of mathematics where

Kenneth Appel (b. 1932) and Wolfgang Haken (b. 1928) had finally solved one of the simplest to state yet most difficult-to-solve problems in the history of mathematics.

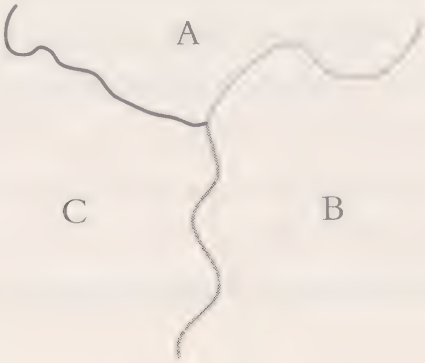


FOUR COLORS
SUFFICE

H Siebert
Abteilung für Mathematik III
Universität Ulm
Oberer Eselsberg
D7900 Ulm
Federal Republic Germany

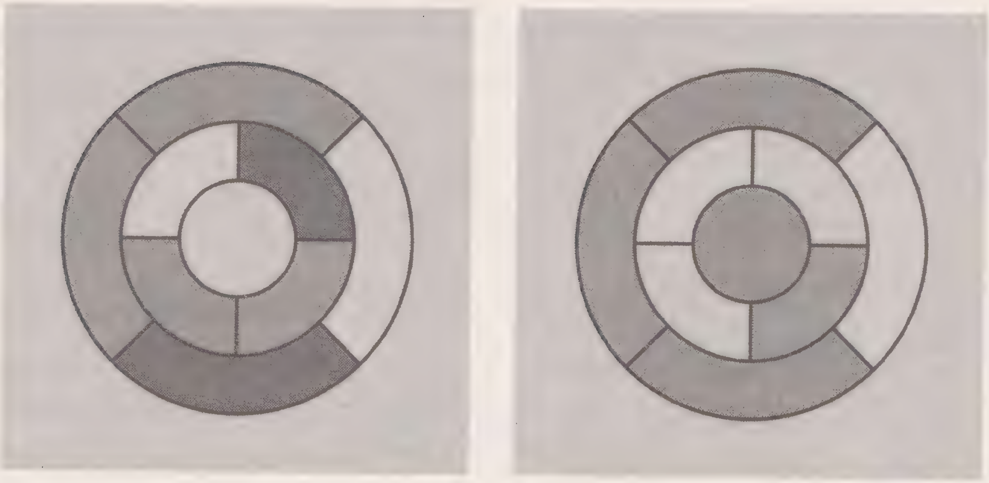
The famous postmark with the words "Four Colors Suffice".

The conjecture – now a theorem – is simply stated thus: "Four colours suffice to colour a conventional planar map in such a way that contiguous regions have different colours". In this case, the term 'conventional' rules out maps in which a single region is divided into non-contiguous areas, as happens with certain enclaves. Nor will we concern ourselves with examples where three countries share a small border crossing point, as in the following diagram.



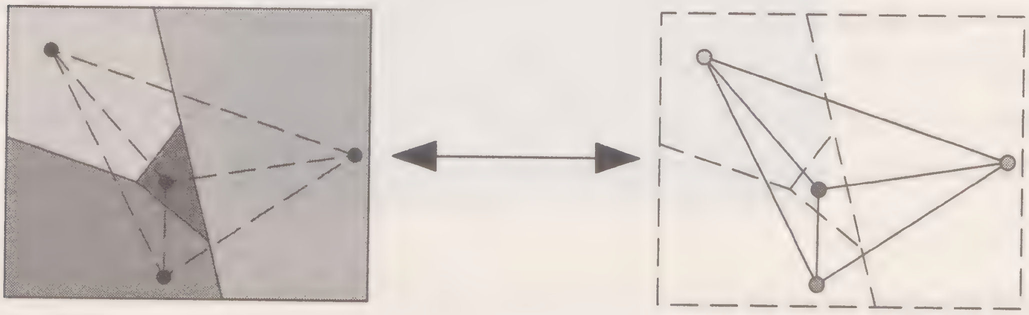
Three countries with a shared border crossing point.

Having said that, the conjecture is stated in very few words and in a somewhat elementary way, yet it is incredibly hard to solve.



The four colour conjecture states that although any planar map may at first seem to need five colours to colour it, it can actually be coloured in four, and that number of colours is sometimes necessary.

The problem was proposed in 1852 by the then lawyer and amateur mathematician Francis Guthrie and entered the scientific world via Augustus de Morgan (1806–1871). There have been a series of false proofs that served above all to show the genuine complexity of the problem and ultimately to locate it within the appropriate field: graph theory. Alfred Kempe (1849–1922) claimed to have found a proof in 1879, which was followed by Percy Heawood's (1861–1955) intervention and the establishment of the 'five colours conjecture' as a theorem (1890). However, the four colours suffice conjecture remained unproven. To reduce the map colouring problem to a graph theory problem, each region has to be replaced by a vertex, and each pair of regions that share a boundary has to be replaced by an edge. The question is how the vertices are coloured, bearing in mind that they may not be the same colour if they are contiguous in a graph, as the following illustrations show.



Little by little, technical concepts emerged such as unavoidable sets and reducible configurations, until Heinrich Heesch (1906–1995) reduced the number of configurations needed to check to 8,900. Kenneth Appel and Wolfgang Haken subsequently reduced this to 1,500 configurations. They had to use a computer to analyse them; a detailed analysis would have been impossible without one.

Once all the configurations were checked, the conjecture was verified and the conjecture became a theorem. Four colours are enough. In more mathematical but less accessible language, for a map on an orientable surface of genus g, N colours suffice and are generally needed;

$$N = \left\lfloor \frac{7+\sqrt{1+48g}}{2} \right\rfloor,$$

where the symbols $\lfloor \quad \rfloor$ denote the 'floor function'. For (orientable or non-orientable) surfaces with positive genus and the topological characteristic χ the formula is as follows:

$$N = \left\lfloor \frac{7+\sqrt{1-24\chi}}{2} \right\rfloor.$$

For planar maps, both formulae produce the result 4.

Appel and Haken's proof was computer-assisted, which wasn't to the liking of some mathematicians because, in principle, a program that runs on one computer may not do so on another, if for no other reason than a tiny programming error. However, there were others who were reticent to accept non-human methods. The incident involving Thomas Nicely and the malfunctioning Intel processor – which we will discuss in more detail later – didn't help to calm the waters. Finally, in 2008 Werner and Gonthier restricted the proof to a universal logical language (Coq), eliminating the need for specific computer programs. We might still doubt the proof, but this would mean ruling out almost all of them.

The perfect graph, key to the science of communications, is closely-linked, although it may not appear so at first glance.

Prime pairs

Prime numbers that come in pairs, in the form $(p, p + 2)$, are given the appropriate name 'twin primes'. This relatively new term was coined by Paul Stäckel (1862–1919). Here are the prime numbers below 1,000:

$(3,5), (5,7), (11,13), (17,19), (29,31), (41,43), (59,61), (71,73), (101,103),$
$(107,109), (137,139), (149,151), (179,181), (191,193), (197,199), (227,229),$
$(239,241), (269,271), (281,283), (311,313), (347,349), (419,421), (431,433),$
$(461,463), (521,523), (569,571), (599,601), (617,619), (641,643), (659,661),$
$(809,811), (821,823), (827,829), (857,859), (881,883).$

Computer-assisted searches have shown that 0.274% of numbers are part of a twin-prime pair. The problem, still unresolved, is whether an infinite number of such pairs exists. Experience seems to indicate that yes, an infinite number exists. In 2009 the pair $65{,}516{,}468{,}355 \cdot 2^{333333} \pm 1$, which has 100,355 digits, was found, and it is a twin-prime pair; the list seems to go on and on. It is widely believed to be never-ending. The other twin primes discovered in 2009 were smaller.

In 2004, the American specialist Richard F. Arenstorf revealed a demonstration of the infinite number of twin primes, but the proof was subsequently shown to contain an error, specifically in lemma 8.

The mathematician duo G.H. Hardy (1877–1947) and J.E. Littlewood (1885–1977), who published many joint articles on number theory, revealed a formula, linked to the density of prime numbers in general, which gives an idea of the distribution and abundance of twin primes $(p, p+2)$.

Godfrey Harold Hardy was not only an exceptional mathematician but also a brilliant writer and philosopher who in A Mathematician's Apology *stated his belief that the study of mathematics was justified only by its beauty, dismissing any utility criterion. In addition to his own achievements, he will also be remembered for raising the profile of the exceptional Indian mathematician Srinivasa Ramanujan (1887–1920).*

If $\pi_2(x)$ denotes the number of primes $p \leqq x$ which have a twin $p + 2$, then

$$\pi_2(x) \approx 2C_2 \int_2^x \frac{dt}{(\log t)^2},$$

where C_2 is a constant, which Hardy and Littlewood deduced from probability criteria, and which equals:

$$C_2 = \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \approx 0.660161815846869573927812110014\ldots$$

It is an infinite product that only extends over prime numbers p. The following table shows the values that are currently known.

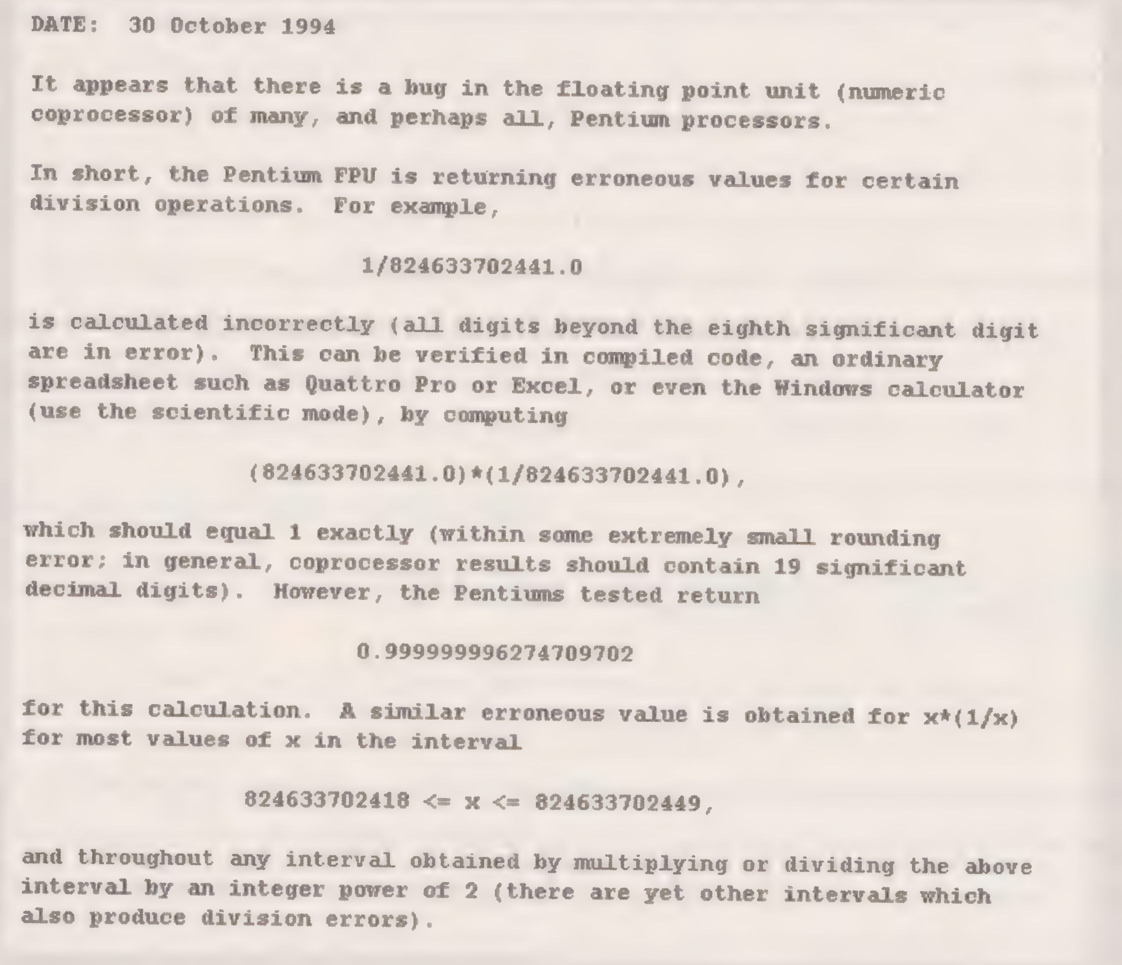
n	$\pi_2(n)$
10^3	35
10^4	205
10^5	1,224
10^6	8,169
10^7	58,980
10^8	440,312
10^9	3,424,506
10^{10}	27,412,679
10^{11}	224,376,048
10^{12}	1,870,585,220
10^{13}	15,834,664,872
10^{14}	135,780,321,665
10^{15}	1,177,209,242,304
10^{16}	10,304,195,697,298
10^{18}	808,675,888,577,436

And the full picture is not so far removed from the small number that we have seen so far, as the following table of twin primes shows.

Gap	Twin primes	
	Expected	Found
100,000,000–100,150,000	584	601
1,000,000,000–1,000,150,000	461	466
10,000,000,000–10,000,150,000	374	389
100,000,000,000–100,000,150,000	309	276
1,000,000,000,000–1,000,000,150,000	259	276
10,000,000,000,000–10,000,000,150,000	221	208
100,000,000,000,000–100,000,000,150,000	191	186
1,000,000,000,000,000–1,000,000,000,150,000	166	161

MAN AND MACHINE

During the course of his research into $\pi_2(x)$, while performing intricate calculations to discover the value $\pi_2(10^{14})$, mathematician Thomas Nicely noticed that, strangely, his computer-based calculations broke down in the interval $824{,}633{,}702{,}418 < n < 824{,}633{,}702{,}449$. So sure was he that the computer was making a mistake that, having ruled out other potential causes, in 1994 he emailed the company that manufactured the microprocessor to warn them, and also warned some of his colleagues. The error was soon identified in the Pentium processor and the renowned firm had to own up, change all the models of the processor in question and improve its quality controls. So, the computer was getting it wrong because one of its components was faulty. Twin primes had finally found their practical application.



DATE: 30 October 1994

It appears that there is a bug in the floating point unit (numeric coprocessor) of many, and perhaps all, Pentium processors.

In short, the Pentium FPU is returning erroneous values for certain division operations. For example,

1/824633702441.0

is calculated incorrectly (all digits beyond the eighth significant digit are in error). This can be verified in compiled code, an ordinary spreadsheet such as Quattro Pro or Excel, or even the Windows calculator (use the scientific mode), by computing

(824633702441.0)*(1/824633702441.0),

which should equal 1 exactly (within some extremely small rounding error; in general, coprocessor results should contain 19 significant decimal digits). However, the Pentiums tested return

0.999999996274709702

for this calculation. A similar erroneous value is obtained for x*(1/x) for most values of x in the interval

824633702418 <= x <= 824633702449,

and throughout any interval obtained by multiplying or dividing the above interval by an integer power of 2 (there are yet other intervals which also produce division errors).

Excerpt from the email that Thomas Nicely sent warning of the error found in a Pentium processor. In the first lines it warns that there seems to be a bug in many of the brand's processors, or perhaps all of them.

This is all beginning to get a little complicated and we don't need to go into the fact that in reality the waters have been muddied still further by parallel conjectures that do not affect numbers separated by two units, but rather by four or more. *Cousin primes* are pairs separated by four units; 'cousin' is used to denote the family link because the fraternal relationship is described by the term 'twins'. Sexy primes are pairs separated by six units, and so on. All of them, 'cousins', sexy primes, etc., can be paired up with unknown values in the same way as twin primes.

A strange feature of twin primes is that if they are turned upside down and added together, the series is convergent, as Viggo Brun (1885–1978) proved:

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{17}+\frac{1}{19}\right)+\ldots\approx 1.902160583104\ldots$$

The opposite happens with conventional primes, where the series of reciprocals diverges:

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{23}+\ldots$$

Conversely, we might assume that there are an infinite number of 'triplet' primes, because as soon as we start looking three come along at once: the numbers 3, 5 and 7 are triplets. But in fact there aren't any more. Primes can be twins but not triplets. And if there aren't any triplets, then it follows that there are no quadruplets, quintuplets, etc.

The Bieberbach conjecture

The personality of Ludwig Bieberbach (1886–1982), a strange Nazi sympathiser who was christened with the middle name Moses, has often obscured the person's talent. He was undoubtedly an excellent mathematician (we'll come back to him later when we discuss Hilbert's problems). Bieberbach's conjecture refers to the holomorphic functions of complex variables, and to their development in power series like the following:

$$f(z) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + \ldots$$

and states that if f maps the unit disk injectively to the complex plane, then

$$|a_n| \leq n|a_1|.$$

If it is given that $a_0 = 0$ and $a_1 = 1$, in which case all the functions can be reduced, an even neater inequality holds true:

$$\left|a_n\right| \leq n.$$

This latter inequality shows, in the analysts' language, that 'the geometric extremity implies metric extremity'.

The story begins with Bieberbach, who proved that $\left|a_2\right| \leq 2$. He then proceeded, step-by-step, with $n = 3, 4, 5$ and 6, until he suddenly had a valid proof for any value of n. The conjecture was finally proven in 1964 by Louis de Branges de Bourcia (b. 1932).

The story would end here were it not for the extraordinary personality of De Branges. There can be no doubt whatsoever about his imagination and mathematical greatness, but he has become an unpopular figure among many of his colleagues. Some of his 'proofs' suffer from the 'boy who cried wolf syndrome', since by claiming so many – and being mistaken – all that De Branges seems to have done is to make many of his peers sceptical. His demonstration of Riemann's hypothesis, for example, is still being checked and therefore remains in limbo. It would take lots of time and energy to check the correctness of a proof that many experts believe is probably flawed. Who would spend years and risk their reputation checking something that may, ultimately, be shot down?

The 100,000-dollar conjecture

With Fermat's last theorem proven, the inevitable consequence was Beal's conjecture, which states that if

$$x^a + y^b = z^c$$

for certain natural numbers x, y, z, a, b and c, with exponents greater than 2, then x, y, z must have a common prime factor. As you can see, it is a generalisation of Fermat's conjecture (now theorem).

It was seemingly first correctly formulated in 1997 by the Texan mathematician Daniel Mauldin. The American banker (and poker player) Andrew Beal (b. 1952) has offered 100,000 dollars for a solution or counter-example, and this prize is still on offer. The sum is not inconsiderable and while solving the conjecture may not merit the front page of the *New York Times*, devoting oneself to such an endeavour certainly brings with it all kinds of satisfactions, including the moral satisfaction of solving a difficult numerical enigma. It is not a category 'one' conjecture, like the Millennium Prize Problems (for which 1 million dollars is on offer), but nor is the reward insignificant.

The following are some results achieved using a computer, but although they satisfy the equation, they also satisfy the conjecture and are not counter-examples.

$$3^3 + 6^3 = 3^5$$
$$3^9 + 54^3 = 3^{11}$$
$$3^6 + 18^3 = 3^8$$
$$7^6 + 7^7 = 98^3$$
$$27^4 + 162^3 = 9^7$$
$$211^3 + 3{,}165^3 = 422^4$$
$$386^3 + 4{,}825^3 = 579^4$$
$$307^3 + 614^4 = 5{,}219^3$$
$$5{,}400^3 + 90^4 = 630^4$$
$$217^3 + 5{,}642^3 = 651^4$$
$$271^3 + 813^4 = 7{,}588^3$$
$$602^3 + 903^4 = 8{,}729^3$$
$$624^3 + 14{,}352^3 = 312^5$$
$$1{,}862^3 + 57{,}722^3 = 3{,}724^4$$
$$2{,}246^3 + 4{,}492^4 = 74{,}118^3$$
$$1{,}838^3 + 97{,}414^3 = 5{,}514^4.$$

Timber! Timber! More timber!

Nowadays, mathematical problems don't have the same aura of mystery and magic that they once did, and are no longer solved with strokes of genius by lone thinkers who might take the decisive final step in their reasoning after reading a letter from a friend. That romantic vision is a thing of the past. Instead of letters, emails are exchanged which deal in very concrete terms with a precise subject, as the mathematical forest is now too dense to get a clear view of anything more than our immediate surroundings. The competition between thinkers – and there are thousands of them – discourages the sharing of secrets. Fermat's theorem, for example, was a surprise insofar as Wiles alternated his own – and formidable – lone research with the regular publication in specialist journals of prudently innocuous results that led most of his colleague to believe that he was engaged in routine day-to-day work, rather than devoting body and soul to a fierce struggle with $x^n + y^n = z^n$. On the other hand, problems now sprout like mushrooms, largely because mathematics has grown up. Naturally, what we don't know outweighs what we do, but we know an increasing amount and it is increasingly difficult to check (and understand). As it is impossible to move between all fields and quote contemporary examples of each, we will conclude with a few typical problems, many unsolved, with the sole and modest aim of providing an overview.

RUSSELL'S PARADOX

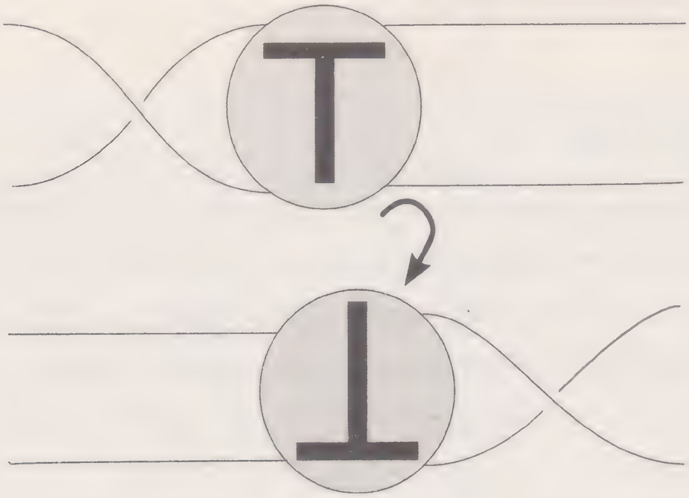
A paradox is, in loose but comprehensible terms, a seemingly reasonable statement that leads to a contradiction. When we enter the territory of logic – and, moreover, of mathematics – we refer to antinomies, rather than simple paradoxes. For example, we describe any set that is not a member of itself as 'normal'; we call 'abnormal' any set that is a member of itself. So, the set A of all sets is abnormal. Consider the set B, which we will define as the set of all normal sets: is B normal or abnormal?

It may at first seem difficult to apply reasoning to it, but after familiarising ourselves with the definition we see that, whatever the answer, there is a contradiction. This is Russell's paradox or antinomy, named after Lord Bertrand Russell (1872–1970), and which he discovered in 1903. The most commonly accepted solution is to reject the intuitive notion of a set and adopt the definition given of the word 'set' in the statement of the Zermelo-Fraenkel axiom, which does not allow for the existence in set theory of objects like A, which proves to be the mother of all conflicts.

A philosopher and mathematician whose work was highly influential on a range of disciplines, Bertrand Russell also campaigned actively for peace and against nuclear weapons, ending up in prison on several occasions.

Tait's conjecture

This conjecture falls within the category of knot theory. It was proposed by Peter Guthrie Tait (1831–1901) and entails the use of the old Scots verb *to flype*, which in modern English translates roughly as *to turn back* and can be represented graphically as follows:



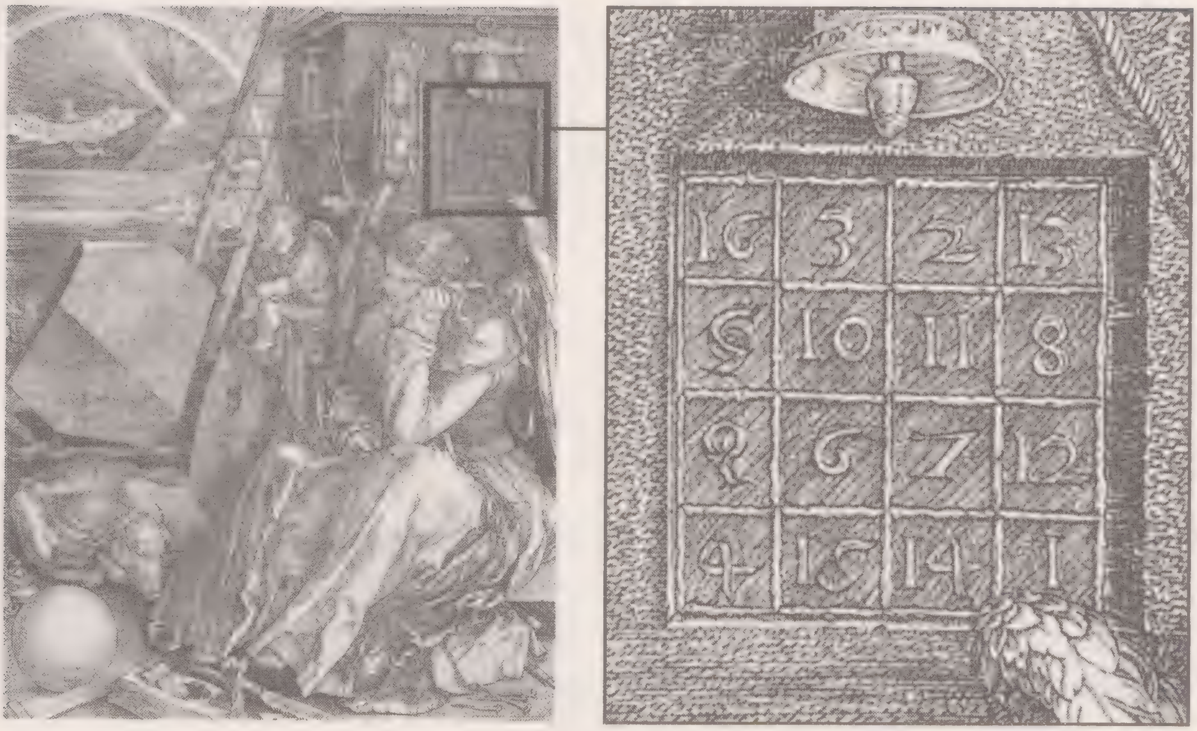
The conjecture, now a theorem, states: "Given any two reduced alternating diagrams A_1 and A_2 of an oriented, prime alternating link, A_1 may be transformed to A_2 by means of a sequence of certain simple moves called *flypes*." It was proven in 1991 by Morwen Thistlethwaite and William Menasco.

Catalan's conjecture

Proposed by Eugene Catalan (1814–1894) and solved positively in 2002 by the Romanian Preda Mihăilescu (b. 1955), it states that of the natural numbers only 2 and 3 have consecutive powers ($2^3 = 8, 3^2 = 9$); specifically 'in $\mathbb{N}$ the only solution of $x^a - y^b = 1$ for $x, a, y, b > 1$ is $x = 3, a = 2, y = 2, b = 3$'.

The prime magic squares conjecture

A flat square array of numbers – i.e. a square matrix – is called magic when its rows, columns and diagonals add up to the same number. The number of boxes per side gives the order of the square. We will now impose the condition that all the numbers must be prime. How many prime squares are there for each order? To date, the question remains unanswered.



An order-4 magic square can be found in Dürer's Melancolia I, *written in the year formed by the two middle numbers in the bottom row: 1514.*

And one final problem

A real number is normal in base 10 when its digits, taken one-by-one, two-by-two, etc., are distributed uniformly. Is π normal? It would be difficult to state a more difficult question in fewer words. This problem has no solution. And we could go on and on, until we dropped, with solved and unsolved mathematical problems.

Chapter 4

Hilbert's Problems

We must know! We will know!
David Hilbert

During the 1900 Congress of Mathematicians, David Hilbert (1862–1943), then regarded as the foremost mathematician in the world, presented a list of 23 unsolved problems, the resolution of which would, he thought, constitute a major step forward for mathematics. Hilbert was the only figure with the authority to set the problems in this way, as he was perhaps the last thinker with the knowledge required to make an informed comment on all branches of mathematics. After Hilbert, no single person would be able to do this. The tree of mathematics is too large and has too many branches. When Hilbert presented his list of 23 problems, he said that a good test for a problem was to present it to the first person you meet in the street. If you could explain it and they could understand it, then it was the perfect problem – it was well formulated. As we will see, either Hilbert was being overly optimistic – or his list of problems is not the same one he read out in 1900.

Many of the 23 problems have now been solved; others – the minority – have remained intractable; and the rest are no longer as relevant and are of little interest today. There are things that will necessarily remain unsaid, since getting to the heart of them, through the jungle of cutting-edge mathematics, would take hundreds of barely comprehensible pages.

Problem 1

The first problem set by Hilbert has become well-known as the continuum hypothesis. The continuum of the title is the number line, the term commonly used to refer to the real numbers. We will take it to mean $\mathbb{R}$. The quickest and easiest way of approaching this question is the intuitive method, which most people can understand, albeit with a certain intellectual effort. Sets can be partitioned very naturally into disjoint subsets that have no common members, referred to as equivalence

A PECULIAR SCHOLAR

Hilbert was the key figure at the University of Göttingen, a supporter of feminism in a male-dominated society and a democrat until his death, condemned to obscurity by the Nazis in his later years. In life he was quite a character, the embodiment of the absent-minded professor. On one occasion, so the story goes, he was hosting a reception and his wife didn't like something he was wearing so sent him to the bedroom to change. He went up to their room and began to change but, unfortunately, his normal routine kicked in: He took off his tie, shirt, etc. His wife came in and, finding him in bed, yelled at him to get up. Hilbert had forgotten all about the party and gone to sleep.

Photograph of David Hilbert taken in 1912, when he was Professor of Mathematics at the University of Göttingen.

classes, by a relationship R called the equivalence relation. When something called x is related to something else called y by means of the relation R we write xRy.

Say R is an equivalence relation if R has three elementary properties:

1. R is reflexive: in other words xRx whatever x *is.*
2. R is symmetric: if xRy, then yRx.
3. R is transitive: if xRy and yRz, then xRz.

An equivalence class of sets determined by R is defined by choosing any one of its members, let's say member a:

$$\text{Class of } a = \{x / xRa\}.$$

In other words, the same class comprises sets that are interrelated by R. Logically, if aRb then:

$$\text{Class of } a = \text{Class of } b.$$

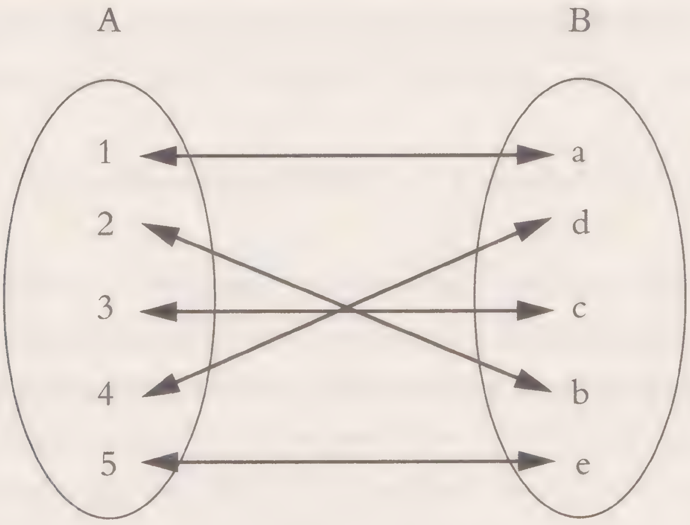
And we see that a class can be identified on the basis of any of its members, which are usually designated class representatives. The classes are not empty (in mathematics we write *Class of a* $\neq \emptyset$), since at the very least, by virtue of reflexivity, $x \in$ *Class of x*.

Distinct classes are disjoint, since if *a* and *b* shared any member, *x*, we would see that:

1. xRa and xRb by definition.
2. $xRa \Rightarrow aRx$ by symmetry.
3. aRx and $xRb \Rightarrow aRb$ by transitivity.
4. *Class of a* = *Class of b* by definition.

And they would no longer be distinct classes.

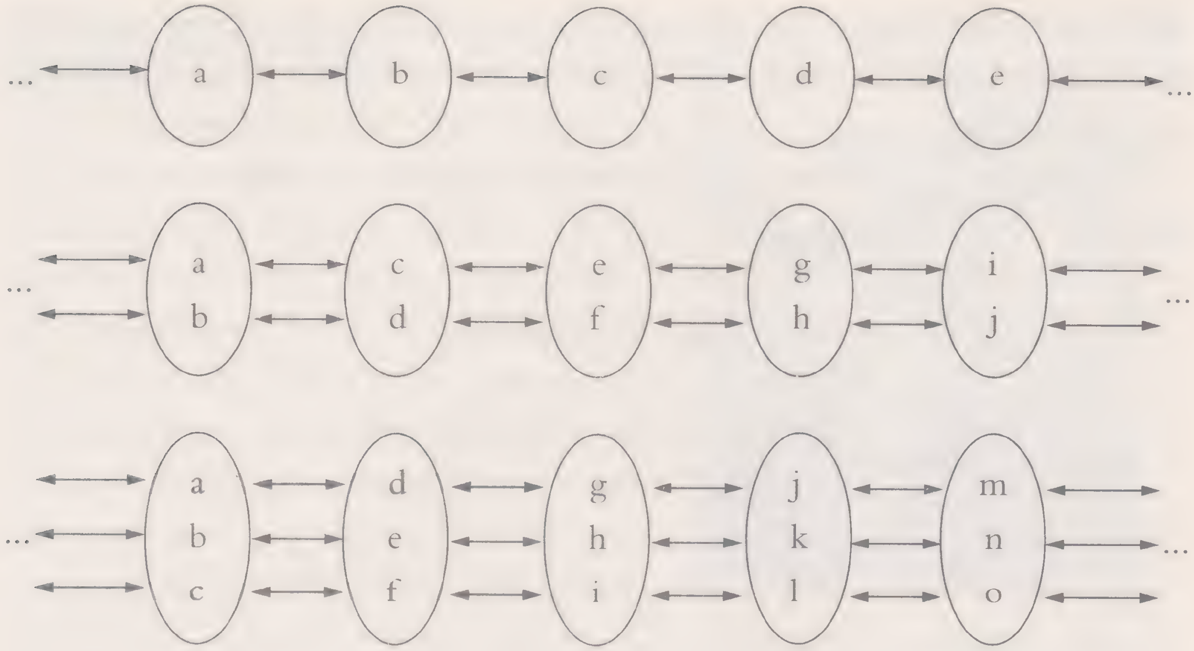
Let's apply all this to the sets. Instead of *R* we will insert the symbol ~, which we will take to mean 'has a one-to-one correspondence with *b*'. We establish the de facto ~ relation very simply; two sets *A* and *B* will be related by ~, and we write $A \sim B$, when a bijective (or biunivocal or one-to-one) correspondence can be established between them:



$A \sim B$

Bijective equivalence between A *and* B.

It's clear even to us mere mortals that the relation ~ defines an equivalence relation between sets. Don't take our word for it. Let's look at a diagram of the resulting classes:



The class of 1, of 2, of 3 and so on.

As you can see, the same class comprises those sets that can have a one-to-one correspondence with each other. Related sets are in the same class; the classes are disjoint and are not empty.

It is legitimate to call each class cardinal; colloquially, we say that the members of each class have the same cardinality. In symbol form, we write and read:

$$\textit{Class of } A = \textit{Cardinal of } A = \#A.$$

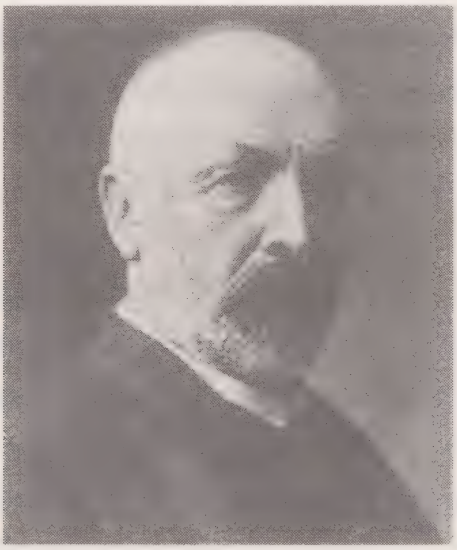
When A is finite, we usually say 'number of members of' rather than 'cardinal of'. It's just a manner of speaking. The cardinal of the $\varnothing$ set is designated by 0 or 'zero'. The most interesting cardinals, because they were discovered most recently and have the most exciting properties, are transfinite or non-finite cardinals.

It is easy to see – like Georg Cantor (1845–1918), the genius who discovered the infinite cardinal – that the first number sets share the same cardinal, which is $\aleph_0$, the first of the cardinals of infinite sets, also called transfinite cardinals.

$$\#\mathbb{N} = \#\mathbb{Z} = \#\mathbb{Q} = \aleph_0.$$

When a set has the cardinal $\aleph_0$, it is said to be countable.

It is also odd, because it seems unexpected, that clearly distinct sets share the same cardinal. Even more surprisingly, the following number set, the real numbers $\mathbb{R}$, which are usually identified with the number line, have the same cardinal as $\mathbb{R}^2$, $\mathbb{R}^3 \ldots, \mathbb{R}^n$. That a space has the same number of points as a line, the same as a square, the same as a cube, etc., is still surprising. When Cantor showed that the cardinal of the points on a line is equal to the cardinal of any space, his contemporaries were sceptical. There is nothing odd about it.



Georg Cantor made great contributions to mathematics, including the concept of infinity and set theory.

The cardinal of $\mathbb{R}$ and its powers, $\mathbb{R}^2, \mathbb{R}^3, \ldots, \mathbb{R}^n$ etc. will be called c.

$$\#\mathbb{R} = \#\mathbb{R}^2 = \ldots = \#\mathbb{R}^n = c.$$

Meanwhile, if $\wp(\mathbb{N})$ denotes the set of the parts of $\mathbb{N}$, we define $\wp^n(\mathbb{N}) = \wp(\wp^{n-1}(\mathbb{N}))$ recursively with $\wp^0(\mathbb{N}) = \mathbb{N}$ and we then define the successive transfinite cardinals, called 'aleph numbers',

$$\#\wp^n(\mathbb{N}) = \aleph_n$$

a perhaps incomplete telescoping series of cardinals of strictly increasing size is created:

$$\aleph_0 < \aleph_1 < \aleph_2 < \ldots < \aleph_n < \ldots$$

We should note here, since they have been mentioned, that there are transfinite numbers of different sizes, some of them very, almost unimaginably, large. They answer to such evocative names as ineffable numbers, huge numbers, *n*-huge numbers, etc.

To any specialist it is quite clear that $c \leq \aleph_1$, but the great unknown, which Cantor could never prove, is:

$$c = \aleph_1.$$

This unproven formulation is the continuum hypothesis, which was solved by Paul Cohen (1934–2007) in 1963. And what is the solution? Well, what Cohen proved is that there is no solution. To understand it, we need to read problem 2, which is linked to the legacy of Kurt Gödel (1906–1978).

Problem 2

What follows will be necessarily brief and not entirely rigorous, because a genuinely understandable and fully correct presentation would be very lengthy indeed. Many popular science books have been written – and will continue to be written – about Gödel's theorem and we will bow to them. What follows is a highly generalist, very simplified presentation that lacks any significant value; it is deliberately elementary.

A theory is expounded on the basis of axioms or initial suppositions; a set of rules of inference moves science forward, generating theorem after theorem, which are deduced from said axioms and rules of inference. This is how mathematics can be advanced, and the theory we call arithmetic is the simplest example, as in principle few theoretical frameworks are required. A theory is consistent when the system's rules of inference cannot be used to demonstrate a statement and its converse. It is not admissible that on the one hand it can be proven that $1 + 1 = 2$ (of course, Bertrand Russell addressed the problem of proving '$1 + 2 = 2$' in paragraph 54.43, p. 379 in Part II of his *Principia Mathematica*), and subsequently that $1 + 1 \neq 2$.

On the other hand, we would like a system of logical connectives that is complete. This means, simply, that given any true statement from the system it should be possible to prove it. For example, $4 + 23 = 27$ should be solvable using arithmetic. Naturally we mean statements within the system, since the statement 'chances are it's Friday and it's raining' may lack significance in, say, arithmetic.

What Hilbert was asking in his second problem is not entirely clear but is along the lines of finding out and proving the consistency of arithmetic, which he considered self-evident but unproven. What Gödel proved in his second incompleteness theorem of 1933 is somewhat surprising: Gödel proved that any axiomatic system that encompasses elementary arithmetic may be consistent, but is necessarily incomplete. This means that armed only with the tools of the system, there will always be true statements that cannot be demonstrated. Naturally, they will still be provable by extending the system (for example, an obvious procedure entails accepting them as axioms), but within the system, nothing can be done. There will always be unprovable propositions. This might well answer Hilbert's second problem, but what about the continuum hypothesis? What about the first problem?

The continuum hypothesis is indeed Gödelian, as Cohen demonstrated. More precisely, Gödel proved that the continuum hypothesis was consistent with elementary set theory based on the Zermelo-Fraenkel axioms, and Cohen demonstrated the negation of said theory was also consistent with the hypothesis. Consequently, it follows that the continuum hypothesis is consistent with elementary set theory whether it is accepted or negated. The continuum hypothesis is an independent statement.

We cannot leave Gödel without noting that the continuum hypothesis is not the only problem that we know of that is undecidable. In the next chapter we will define what a Turing machine is; we will then encounter (but won't dwell on) another undecidable question. The problem of knowing in advance whether any Turing machine, once switched on, will ever stop or whether this too is undecidable.

A COMPLICATED CHARACTER

Gödel was an extraordinary man, as sharp and profound in his scientific reasoning as he was paranoid and manic in his daily life – especially in his later years. Born in Czechoslovakia, he was persecuted by the Nazis and took U.S. citizenship – with difficulty as he tried to dispute the logical wording of the Declaration of Independence with the judge who was approving his application. His death gives us an insight into his complicated personality. He feared being poisoned and only ate food prepared by his wife, the only person he trusted. However, when his wife was hospitalised in old age, Gödel starved to death!

Kurt Gödel was renowned for his work on logic and set theory.

Problem 3

This problem consists in rigorously demonstrating that two tetrahedra of equal base and height – but not form – have the same volume. But, and herein lies the difficulty, without using Archimedes' axiom, which characterises the field $\mathbb{R}$: If $a < b$ and $a, b \in \mathbb{R}$, there exists an n such that $na > b$.

Few people believe that Archimedes discovered all this. What Hilbert was looking for were two tetrahedra like those described, but such that the first could be cut into a finite number of congruent pieces which, reassembled in some way, could be used to construct the second. Such tetrahedra do not exist, as Max Dehn (1878–1952) demonstrated in 1902.

Problem 4

Hilbert's original requirement was to construc all the metrics, the lines of which are geodesics. Luckily for all concerned (anyone who can read or write), the request is too vague and ethereal. In reality, there can be no concrete solution to a problem stated in this way.

Problem 5

To what extent is differentiability necessary when designing continuous transformation groups, now known as Lie groups? This isn't a vaguely stated problem like the last one, but neither is it a central problem.

The contributions of John von Neumann (1903–1957), Andrew Gleason (1921–2008), Deane Montgomery (1909–1992), Leo Zippin (1905–1995) and Hidehiko Yamabe (1923–1960) resolved the problem.

Problem 6

Axiomatise all of physics. This has been partially completed, but the emergence of new theories (quantum physics, theory of relativity) has made the problem unexpectedly complicated, more so than Hilbert could have predicted. There is value in such an axiomatisation, but it is not now a priority, as there are other more interesting unanswered questions.

Problem 7

Consider the numerical expression a^b, where a is algebraic ($a \neq 0$ or 1 for obvious reasons) and b is irrational. Is a^b transcendental? Two number theorists, Alexander Gelfond (1906-1968) and Theodor Schneider (1911-1988) demonstrated independently and almost simultaneously, in 1934 and 1935, what is now known as the Gelfond-Schneider theorem. It states: "If a and b are complex numbers, with a algebraic and b irrational, any value of a^b is transcendental." The "any value" refers to the fact that, when a and b are complex, a^b is a complex power and, like many complex powers, allows many solutions.

This theorem corresponds exactly to the question of transcendence set by Hilbert. In particular, a corollary of the Gelfond-Schneider theorem is the transcendence of $2^{\sqrt{2}}$, e^{π} o i^i, which had long been conjectured.

Problem 8

This is the Riemann hypothesis, the only one of the 23 problems to be included on the list of Millennium Prize Problems by the Clay Institute. We will discuss it in the next chapter.

Problem 9

This consists in finding the most general reciprocity law possible in an algebraic number field. The reciprocity law, which had major repercussions in the 19th century, is expressed using the Legendre symbols, $\left(\frac{n}{p}\right)$, which function as follows:

$$\left(\frac{n}{p}\right) = 0 \text{ if } n \equiv 0 \pmod{p},$$

$$\left(\frac{n}{p}\right) = +1 \text{ if } n \not\equiv 0 \pmod{p} \text{ and } x \text{ exists such that } x^2 \equiv n \pmod{p},$$

$$\left(\frac{n}{p}\right) = -1 \text{ in other cases}$$

And this is the departure point for a whole system of computational calculus, which provides numerous useful formulae, notably:

$$\text{If } p \text{ and } q \text{ are odd primes, } \left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

known as the 'golden theorem' since the time of Gauss, who was a devotee of such expressions. Gauss proved that

> "For any two odd primes such as p and q,
> $-q$ is a square (mod p) $\Leftrightarrow$ p is a square (mod q)
> except when both are of the form $4n-1$, in which case
> $-q$ is a square (mod p) $\Leftrightarrow$ p is not a square (mod q)."

The quadratic reciprocity law sought by Hilbert was developed by Emil Artin (1898–1962) during the period 1924–1930 and is a hugely elegant theory (like anything associated with Artin) in which ideals replace ordinary numbers.

Problem 10

This aims to find a procedure or algorithm to determine whether a Diophantine equation is solvable or not. It is a question of decidability which falls squarely within what have come to be called 'mass problems', since the decision, whether the answer is yes or no, affects many cases – infinitely many, in fact – and not one or more specific cases. Clearly, there are Diophantine equations for which there is a known solution algorithm, but the question is whether there is a single algorithm that applies to all. Martin Davis (b. 1928), Julia Robinson (1919–1985) and Hilary Putnam (b. 1926), worked on this problem and made significant headway, but it was left to the young but prodigious Russian Yuri Matiyasevich (b. 1947) to prove the final yet crucial step (1970). Incidentally, he used as a key element in his reasoning a Diophantine equation based on the Fibonacci numbers. It is also worth noting that Matiyasevich's conclusion (which states that "all recursively enumerable sets are Diophantine") is equivalent to Gödel's incompleteness theorem.

Problem 11

This one focuses on solving quadratic forms with algebraic coefficients. Just to be clear, a quadratic form $\mathbb{Q}(x_1,x_2,...,x_n)$ in n variables over $\mathbb{R}$ is the most common, and is a polynomial of degree two

$$\mathbb{Q}(x_1, x_2, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$$

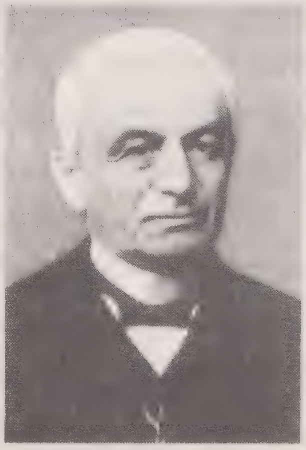
with $a_{ij} \in \mathbb{R}$. Although amply studied in the fields $\mathbb{R}$ and $\mathbb{C}$, the same work remained to be done in $\mathbb{Q}$ and, for example, in the *p*-atic fields $\mathbb{Q}_p$. Helmuth Hasse (1898-1979) and Carl Siegel (1896-1981), both German, devoted their energies to the remaining cases. Incidentally, Hasse, who was of Jewish origin, applied for Nazi party membership in 1937, demonstrating that being a mathematician is not a precondition for being intelligent. Siegel, meanwhile, was vehemently anti-Nazi.

Problem 12

Leopold Kronecker (1823-1891) claimed that as a young man he had dreamt of solving Abelian extensions, imaginary quadratic fields, algebraic numbers, field extensions, cyclotomic roots and various other algebraic phenomena with tenuous links to reality. Hilbert, albeit a little incoherently, brought them together in his 12th problem, generalised them and put them forward as an important question to be resolved. In 1886 the Kronecker-Weber theorem referred the Abelian extensions to the field of rational numbers, $\mathbb{Q}$, as sub-fields of a cyclotomic field (in other words, of roots of unity) and Kronecker's dream was seemingly to extend the said result to any field *K*, whether

AN ORIGINAL MATHEMATICIAN

Leopold Kronecker was an original mathematician by modern standards. He will be remembered as a fine professional who made a great contribution to mathematics, but he was also excessively meticulous, unshakeable in his constructivist beliefs, and had absolutely no time for thinking that departed from primordial intuition. He is famous for saying: "God made natural numbers; all else is the work of man". With such convictions it comes as no surprise that Kronecker opposed, sometimes quite brutally, the ideas of visionaries such as Cantor and his followers.



Leopold Kronecker's name is now associated with various mathematical formulations, notably the Kronecker–Weber theorem.

or not it was the famous $\mathbb{Q}$. This was the progress sought in proposing problem 12.

The question is not a central concern today and no fully adequate theory has been proposed.

Problem 13

We know that any equation of degree five or higher cannot be solved using roots alone. Hilbert asked whether, using the much more general functions of two variables, there was a valid solution for any 7th-degree equation. Explained in this way, it all seems a little senseless, so we will try to explain the significance.

Firstly, it is not clear that there really are functions of three variables. The most simple often-cited example is that of the sum function $f(x, y, z) = x + y + z$ which can be easily reduced to a composition of functions of two variables just by putting $f(x, y, z) = x + (y + z)$.

Hilbert knew that equations of degree 5 and 6 allowed simplified propositions and turned his attention to the version of the 7th-degree equation given by the then irreducible expression of the form:

$$x^7 + \alpha x^3 + \beta x^2 + \chi x + 1 = 0,$$

with three variables, α, β and χ. One solution to this polynomial should be a continuous function of these three variables. Could this be simplified to give a solution composed of functions of two variables?

It was clear that if anyone proved that any continuous function of three variables could be reduced to a finite composition of continuous functions of two variables, it would settle the question, although this was more than Hilbert had asked for. Indeed, this was proven, in 1957 and in successive stages, by Andrei Kolmogorov (1903–1987) and Vladimir Arnold (1937–2010). In fact, they proved even more: Any continuous function of several variables can be constructed with a finite number of two-variable functions.

Some say that Hilbert did not mean continuous functions, but rather algebraic functions (in other words, polynomials with polynomial coefficients) and that the problem has therefore not been solved. If Hilbert was indeed referring to these functions, then the problem is still open.

Problem 14

Problem 14 is a complex algebraic question concerning invariant theory. From a geometric perspective, it affects manifolds and subvarieties of the same generated by intersection with others, which exhibit a specific finitely generated structure (polynomial) and 'transmit' it to the original variety. The development of the question, of mathematical interest to experts but difficult to explain, seemed in principle to follow Hilbert's intuition, but took a definitive twist when the shrewd Japanese mathematician Masayoshi Nagata (1927–2008) discovered a counter-example to the problem and settled it for good in 1958.

Problem 15

Schubert calculus, a cross between combinatorics and algebraic geometry, is not a very accessible subject. Specialising in it requires a huge intellectual effort. Some people say it takes three times as much time and knowledge to work in this field as in other fields. The German mathematician Cesar Hannibal Schubert (1848-1911) laid the foundations for this form of calculus, which essentially boils down to describing the multiplicative structure of a cohomology ring. Unfortunately, this description resembles Giovanni Papini's description of *The Odyssey*: "The erratic and interminable adventures of a poor fool who could never remember where he lived." The theory on which this complicated calculus was based was not mature enough and it was not until the mid-20th century that more rigorous frameworks were developed that moved us on to firmer ground.

What Hilbert wanted to do was justify Schubert calculus and therefore the problem can only be said to have been partially solved. With respect to the calculus itself, the picture seems clear, although very complicated. As regards so-called enumerative geometry, the branch of geometry that underpins the calculus, a lot of work remains to be done.

Problem 16

Hilbert's original formulation divides the problem into two parts and states the question in fairly vague terms, although he was referring to real objects, such as ovals originating from certain real algebraic curves (in projective space) and Poincaré limit cycles of planar vector fields. Nonetheless, Hilbert's actual statement of what he was looking for is too vague and many think the problem comes down to something as nebulous as studying the topology of curves and real algebraic surfaces, a legitimate yet generic ambition which, as such, remains to be achieved. Indeed, there is no prospect of it being achieved soon because of its sheer scope.

Both parts of problem 16, in their strict interpretations, are regarded as being in an advanced stage of research, with possible but unconfirmed solutions.

Problem 17

A rational function f is, to be clear, a polynomial quotient with real coefficients:

$$f(x_1,x_2,...,x_n)=\frac{P\ (x_1,x_2,...,x_n)}{Q\ (x_1,x_2,...,x_n)}$$

Such functions determine a field. When $x_1,x_2,\ldots,x_n$ are assigned a value (except the zeros of the denominator), $f\ (x_1,x_2,\ldots,x_n)$ in turn takes on another value, which may be positive or negative. In some cases, all the values of $f\ (x_1,x_2,\ldots,x_n)$ are positive. Hilbert wondered, naturally, whether $f\ (x_1,x_2,\ldots,x_n)$ could be expressed in this case as a sum of squares of rational functions.

In the field of numbers, we already know (as Lagrange discovered) that any natural number n is the sum of no more than four squares, repeated or otherwise. Hilbert was looking to somehow generalise this simple result.

This was one of the problems that fortune smiled most warmly upon. The young and brilliant Emil Artin solved it in 1927, and his first proof runs to just fifteen pages.

Artin was not really worried whether his proof as – in keeping with the laws of intuitionist purism – a constructive proof. In fact, Artin demonstrated the problem in the affirmative, but did no more than that. He didn't show how to construct the functions of the sum of squares or worry about how many solutions there were. We had to wait many years for Charles Neal Delzell, from the University of Louisiana, to find a rigorous construction algorithm. But even now that we have an algorithm, we still cannot say how many squares of rational functions are needed. We only know that this number is less than 2^n where n is the number of variables.

Problem 18

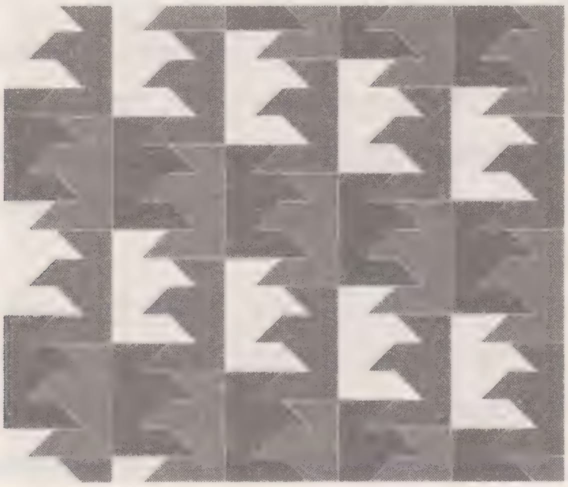
Hilbert's 18th problem is really three problems in one. In making his speech, Hilbert got a little carried away and grouped together questions he regarded as related, although in reality they are quite separate.

Part one. We know that in two dimensions there are 17 symmetry groups, as independently proved by Evgraf Fedorov (1853-1919) and George Pólya (1887-1985). We also know that in three dimensions this figure rises to 230; the crystallographers resolved this (there are various methods of counting and various equivalent results). Fedorov is regarded as the man chiefly responsible for this number. The question now is what happens in *n* dimensions.

The answer was delivered by Ludwig Bieberbach (1886-1982) in *Über die Bewegungsgruppen der Euklidischen Räume* (*On Groups of Movements in Euclidean Space*), published in 1911. The number of symmetry groups in *n*-dimensional space is finite for any *n*, which was the answer to Hilbert's question. For $n = 4$ there are 4,895 crystallographic groups – found using a computer – and for $n = 6$ there are 28,934,974; for many other values of *n* the exact number is unknown, since no miraculous formula has been found that can tell us. As we noted in the previous chapter, Bieberbach was a Nazi sympathiser who believed in things like 'German science' and its superiority over all other forms of science, which were by definition inferior. This led, at the end of World War II, to his dismissal from all his academic positions in Germany.

Part two. We know that there are polyhedra that tile in space. They do so transitively, or in more precise geometric terms, there are isohedral tilings. This means, in plainer language, that we can always isolate a basic element of the tiling and move it – without rotation, without symmetry – until it matches itself in another position, with the whole tiling of the linked space remaining valid. An anisohedral tiling does not satisfy this condition. The distinction is quite subtle and to understand it fully we need the concept of the symmetry orbit of an element. We might attempt to explain this as follows. It could be that when isolating an element and moving it, the element in question and its orbit matches other pre-existing identical elements, but the other elements outside the orbit do not. Hilbert's question was: is there an anisohedral tiling of three-dimensional space? He probably hoped that, if the problem was resolved, the answer to this question was sometimes 'no'.

Well, Karl Reinhardt, (1895–1941) in *Zur Zerlegung der euklidischen Räume in kongruente Polytope* (*Dividing the Euclidean Space into Congruent Polyhedra*; 1928), demonstrated a polyhedron that solved Hilbert's problem, but in a way which dashed his hopes. What's more, Reinhardt predicted an anisohedral tiling in two dimensions. This prophesy came true in 1935 when Heinrich Heesch (1906-1995) found the tiling below.



Part three. This is perhaps the most interesting section. It concerns the Keplerian problem we have already discussed and which was not solved until the 21st century: sphere packing.

Problem 19

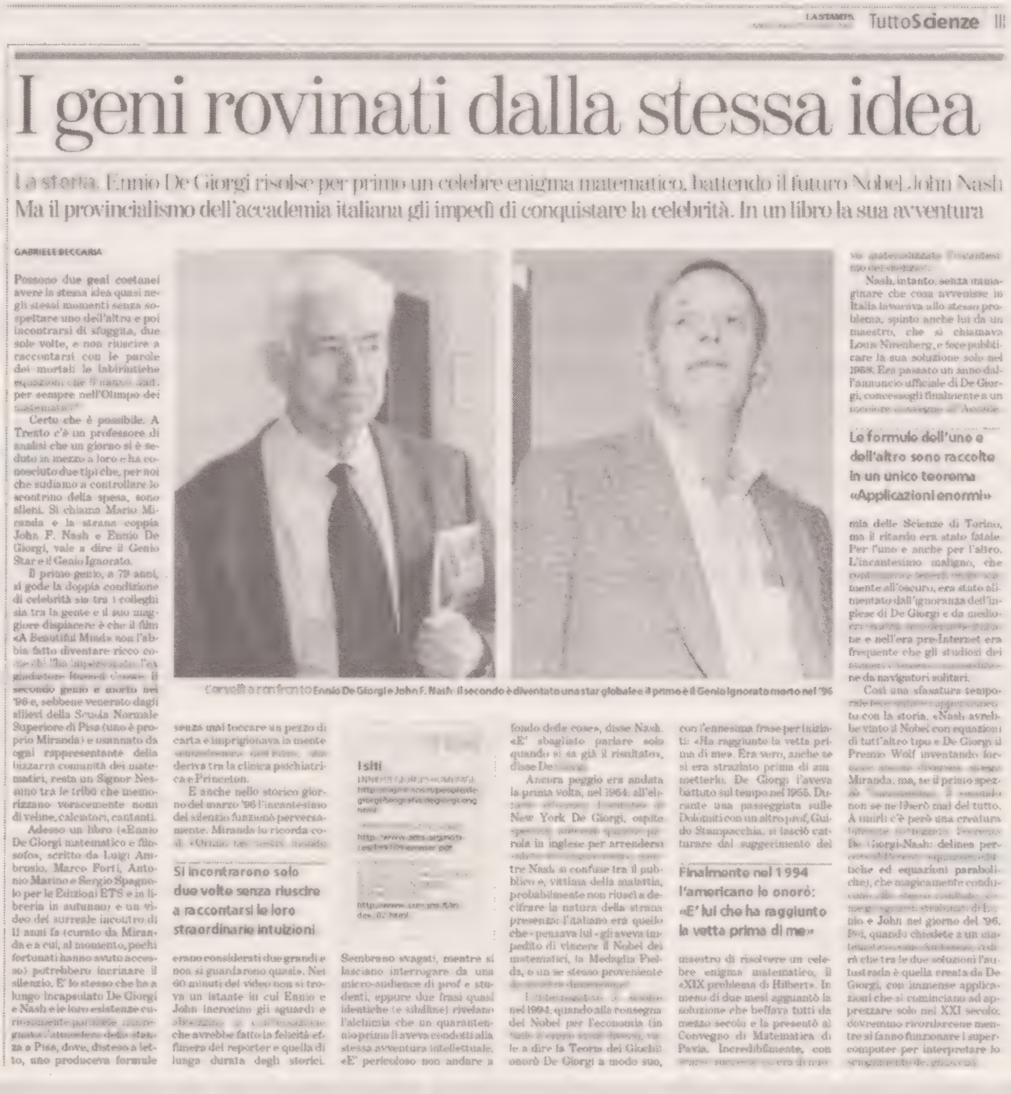
Hilbert asked whether solutions of Lagrangians are always analytic functions. This question is quite technical and has been probed with some success by the experts. Almost immediately, in 1904, the Russian Sergei Natanovic Bernstein (1880–1968) solved the problem in the affirmative, albeit while imposing a number of initial conditions that did not seem too significant. However, they were, and we had to wait until 1956 for the Italian Ennio de Giorgi (1928–1996) to deliver a proof with no limitations.

Problem 20

Calculus of variations is an essential part of analysis, although not of calculus itself, which would be limited to studying functions; instead it forms part of a broader field, that of functionals or functions of functions. The typical calculus of variations problem involves, in a simple example, an integral of the following type:

MATHEMATICS WITH PERSONAL CONSEQUENCES

De Giorgi was a charming personality, a genuine self-made man, deeply religious, an untroubled character and a prominent member of Amnesty International. These qualities did not stop him inadvertently pushing the brilliant Nobel Laureate John Forbes Nash (b. 1928) to the brink of despair and madness. Like De Giorgi, Nash was working on a definitive solution to Hilbert's 19th problem, and the Italian was a few months ahead of him. Viewed with hindsight, De Giorgi provided the first full proof, and Nash – they say – the most elegant. What is certain is that shortly after the publication of the proofs, Nash was diagnosed as a paranoid schizophrenic.



LA STAMPA TuttoScienze III

I geni rovinati dalla stessa idea

La storia. Ennio De Giorgi risolse per primo un celebre enigma matematico, battendo il futuro Nobel John Nash
Ma il provincialismo dell'accademia italiana gli impedì di conquistare la celebrità. In un libro la sua avventura

GABRIELE BECCARIA

Cervelli a confronto Ennio De Giorgi e John F. Nash: il secondo è diventato una star globale e il primo è il Genio Ignorato morto nel '96

Le formule dell'uno e dell'altro sono raccolte in un unico teorema «Applicazioni enormi»

Si incontrarono solo due volte senza riuscire a raccontarsi le loro straordinarie intuizioni

I siti

Finalmente nel 1994 l'americano lo onorò: «E' lui che ha raggiunto la vetta prima di me»

Scripta Volant, Verba Manent, a book on De Giorgi containing contributions from various authors and discussed in this article from the Italian newspaper La Stampa, *details the Italian mathematician's relationship with John Forbes Nash, and the intrigues that prevented him from achieving acclaim after solving Hilbert's 19th problem before anyone else.*

$$\int_a^b F(f(x), f'(x), x)\,dx,$$

in other words, an integral of a function which is a function of another/other function(s) and their derivative(s). The function, in the most general case, may be multivariate, and the derivatives may be partial and non-linear. Calculus of variations deals with maximising or minimising the integral or identifying its regions of stability; in other words, finding its extreme and recurrent sets of singularities to subject them to variations.

Needless to say, since the heroic times of the brachistochrone problem plenty of water has flowed under the bridge of mathematical analysis and calculus of variations has developed enormously. When Hilbert formulated problem 20, he did so at a propitious moment, when a lot of people were interested in it. Hilbert focused on a particular aspect of calculus of variations: boundary conditions. When the function *f* is forced through a specified region, or its derivative (more precisely its derivative vector) is forced to travel along a specific path, we refer to the establishment of boundary conditions and the obligation to respect conditions at the boundary. Dirichlet, Neumann and Robin conditions are well known to experts.

When they are satisfied, there is a solution and the function sought proves to be analytic. Hilbert wondered whether this would always be the case; whether there would always be a solution given reasonable boundary conditions.

Calculus of variations was one of the most intensively cultivated fields throughout the 20th century, and we can confirm that the answer has been found, that it is affirmative and that there are so many names associated with this very general topic that it would be impossible to mention them all.

Problem 21

Monodromy is taken to be a research procedure specific to analysis that consists in 'running round' the singularities of a rational function – the points at which its value becomes infinite – with curves which, in some mysterious mathematical way, encode the secrets of those singularities. Let's imagine a real situation and try to solve a differential equation (or even better, a system of such equations) of the following type:

$$\sum_{k=0}^{n} P_k(x)\frac{d^n y}{dx^n}$$

where P are polynomial functions that exhibit a certain singularity. Suppose, then, that we start at one and proceed along paths around the singularities; this generates groups of matrices between the solutions which constitute the monodromy groups. As you can see, this is all very simple and obvious, with no unexpected concepts or complications...

Inspired by Riemann's work, Hilbert asked whether any group regarded as a monodromy group corresponded to a specific differential equation or system of differential equations. In theory, it was solved in the affirmative in 1907 by the Slovenian mathematician Josip Plemelj (1873-1967). However, there was an error in the proof (in fact, Hilbert did not present the problem sufficiently clearly) and the matter had to be reconsidered in the 1980s. In 1989 the Russian Andrei Bolibruch (1950-2003) found a counter-example to the general case and overhauled the whole theory. Problem 21 can be considered solved, but the answer is 'yes' or' no' depending on the case in question. This question gives rise to Fuchsian functions, named after Lazarus Fuchs (1833-1902), a pupil of Klein. You'll note that we haven't even mentioned them so as not to complicate matters.

Problem 22

If we told you that problem 21 might be considered slightly more general than problem 22, you might breathe a sigh of relief, but don't get your hopes up. Problem 22 deals with uniformisation, a question that relates to mathematical analysis. Stated somewhat hastily and loosely so that we can grasp the concept, say we take the example of a planar circumference with real points $x^2 + y^2 = 1$, centred on (0, 0) and a unit radius. Its parameters can be set with the help of the trigonometric functions, characterising its points as those with coordinates of the form $(\cos\alpha, \sin\alpha)$ for an $\alpha \in [0, 2\pi]$; but they can be set more elegantly using rational functions giving

$$\left(\frac{2\lambda}{1+\lambda^2}, \frac{\lambda^2-1}{\lambda^2+1}\right) \text{with } \lambda \in \mathbb{R}.$$

An expression of this type is called uniformisation of the actual circumference. This process also operates in the world of complex numbers $\mathbb{C}$ and Poincaré proved that it was universally valid for those functions where the relationship between variables is algebraic. Hilbert asked whether this result was always possible; whether the relationship was algebraic or not.

Paul Koebe (1882-1945) and Henri Poincaré solved problem 22 in 1909, and just nine years after it was set it could already be regarded as theoretically proven in the affirmative.

Problem 23

You'll be glad to know, if you've made it this far, that problem 23 was too vaguely – or too ambitiously – stated for it to be regarded as a genuine question. Hilbert made problem 23 an extended exposition in which, in short, he asked what future developments could be expected in calculus of variations. As the question belongs more properly to the field of guesswork than science, this problem will not be considered.

Chapter 5

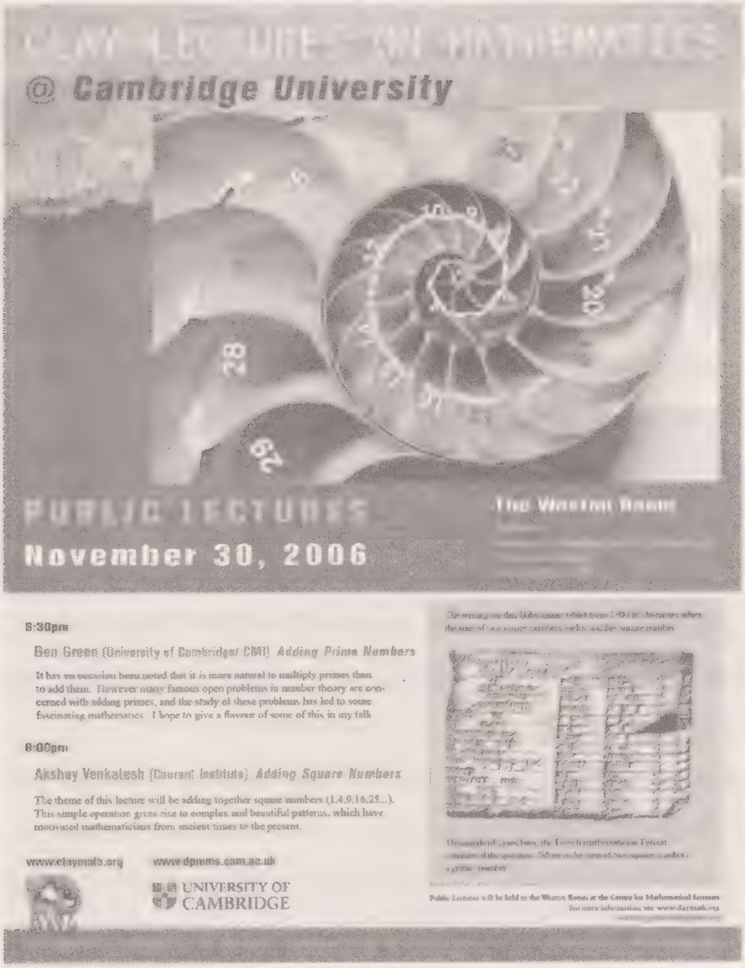
The Clay Problems

The formulation of a problem is often more essential than its solution.
Albert Einstein

The state of mathematics in the 21st century reflects the extraordinary progress made in the preceding centuries. Tens of thousands of articles are published in specialist journals every year, a strong sign of the vitality of this field. There are many incentives for mathematical progress, in the form of jobs, prizes and prestige; the columnist, writer and mathematician Keith Devlin recently wrote that in the United Kingdom a car maker had subsidised a mathematician's research into the geometry involved in the action of parking a car.

These are signs of rude health, and the experts are not unduly concerned, as the idea that mathematics is edging away from salary structures and towards the advancement of knowledge seems to be gaining traction little-by-little. The problems mathematicians are tackling in the 21st century are multiple and varied, and the more people there are cultivating the field, the more unknowns are dug up and need settling. Nonetheless, a certain consensus is emerging on the questions that are truly fundamental. It is believed that solving these questions will move the whole field forwards and shine light into all corners. Naturally, perhaps not all the predicted progress has been made, but there have been notable advances.

The Clay Mathematics Institute set itself the task of classifying these fundamental problems and promoting their resolution. In 1998 the millionaire American philanthropist Landon T. Clay, with the help of his wife Lavinia and Professor Arthur Jaffe (b. 1937) of Harvard University, founded the Clay Mathematics Institute in Cambridge, Massachusetts. At the same time, he endowed his foundation with enough money to offer a series of generous prizes and research incentives, which gave rise to seven prizes of a million dollars each for whoever solved what the committee of experts termed 'The Millennium Problems'. This is a very limited set of problems which, unlike in the past, are not associated with the intellectual interests of a single thinker, eminent though Hilbert was. In a nutshell, the seven problems chosen by the institute might be considered 'the magnificent seven' of the science of pure thought. *La crème de la crème.*



CLAY LECTURES ON MATHEMATICS

@ Cambridge University

PUBLIC LECTURES

November 30, 2006

5:30pm

Ben Green (University of Cambridge/ CMI) *Adding Prime Numbers*

It has on occasion been noted that it is more natural to multiply primes than to add them. However many famous open problems in number theory are concerned with adding primes, and the study of these problems has led to some fascinating mathematics. I hope to give a flavour of some of this in my talk

6:00pm

Akshay Venkatesh (Courant Institute) *Adding Square Numbers*

The theme of this lecture will be adding together square numbers (1,4,9,16,25...). This simple operation gives rise to complex and beautiful patterns, which have motivated mathematicians from ancient times to the present.

www.claymath.org

www.dpmms.cam.ac.uk

UNIVERSITY OF CAMBRIDGE

Poster for one of the many events organised by the Clay Institute.

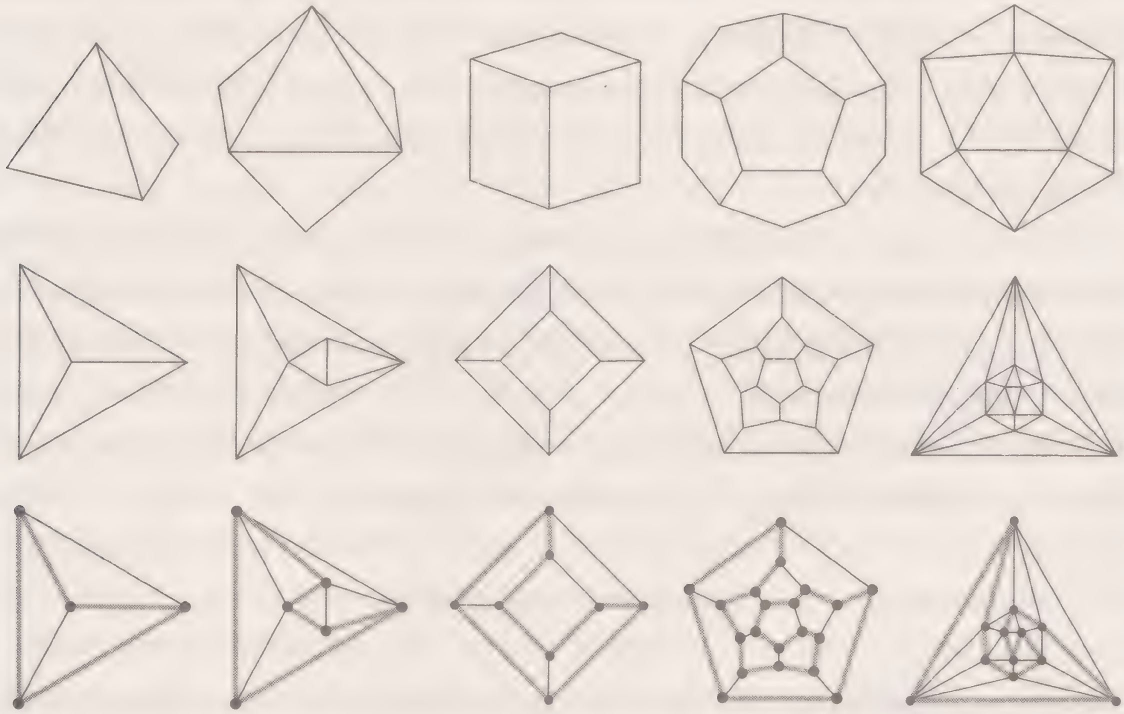
Shortly after the announcement of the problems that were poised to revolutionise research for the next thousand years, the Russian mathematician Gregori Perelman (b. 1966) revealed the solution to the first, the Poincaré hypothesis. A degree of unease was felt in the world of mathematics: what if after so much effort to define the major challenges of the millennium, in just a few years – perhaps just a century – those challenges were no more? So much the better, frankly. Our great-grandchildren will identify their own list of problems to be tackled.

A certain apprehension is also felt by anyone who has to explain the Millennium Problems. Some can be rendered comprehensible in more-or-less plain language, but not others. Mathematical language is now a complex instrument, a repository for a huge amount of information. Any statement in mathematical terms relies heavily on prior knowledge, and many questions stated in just a few symbols actually stand for very complicated concepts which can sometimes be incomprehensible to anyone who is not an expert in the particular jargon they use. In fact, some Millennium Problems take a significant portion of a thousand years just to understand, let alone explain...

P versus *NP*

Solving a problem is not the same thing as checking a possible solution. And in some cases, the difference is considerable. For example, take the school admin task, abandoned many times without finding a solution, of designing a rota of timings and classes that balances the time each teacher has available against the need to put together timetables that work for everyone, and respects each teacher's preferences. If you manage to pull off this infernal calculation, checking whether a solution is valid may seem like child's play. Calculating may be torture, but it's nothing compared with checking the result of the calculation.

Let's take a more mathematical example: a path in a graph is Hamiltonian when it passes through each vertex once. For example, Platonic solids viewed as graphs are all Hamiltonian:



Hamiltonian paths in Platonic polyhedra. Below each polyhedron is the corresponding equivalent graph, and below that, the path.

Searching for a Hamiltonian path in a random graph – not the ones above, which are easy – might be a very long, demotivating task. And yet, should you find one, checking that it is indeed Hamiltonian is easy; it's patently obvious.

The first of the Clay problems can be defined in plain language: can every problem the solution of which can be quickly verified also be quickly solved? Think of a number and a possible divisor; is it an exact divisor or not? It can be checked straight away, by dividing. But actually finding the divisor in the first place is a different kettle of fish. If the departure point is a product of enormous primes and their factors are unknown, finding them is an immense task. In fact, modern public key cryptography relies on it being so difficult that it could take aeons.

We call P the set of problems that are quickly *solvable* and NP the set of problems that are quickly *checkable*. The Clay Institute presents the P *versus* NP problem almost informally; it states:

$$\text{Is } P = NP?$$

It was stated by Stephen Cook, who introduced the problem in 1971.

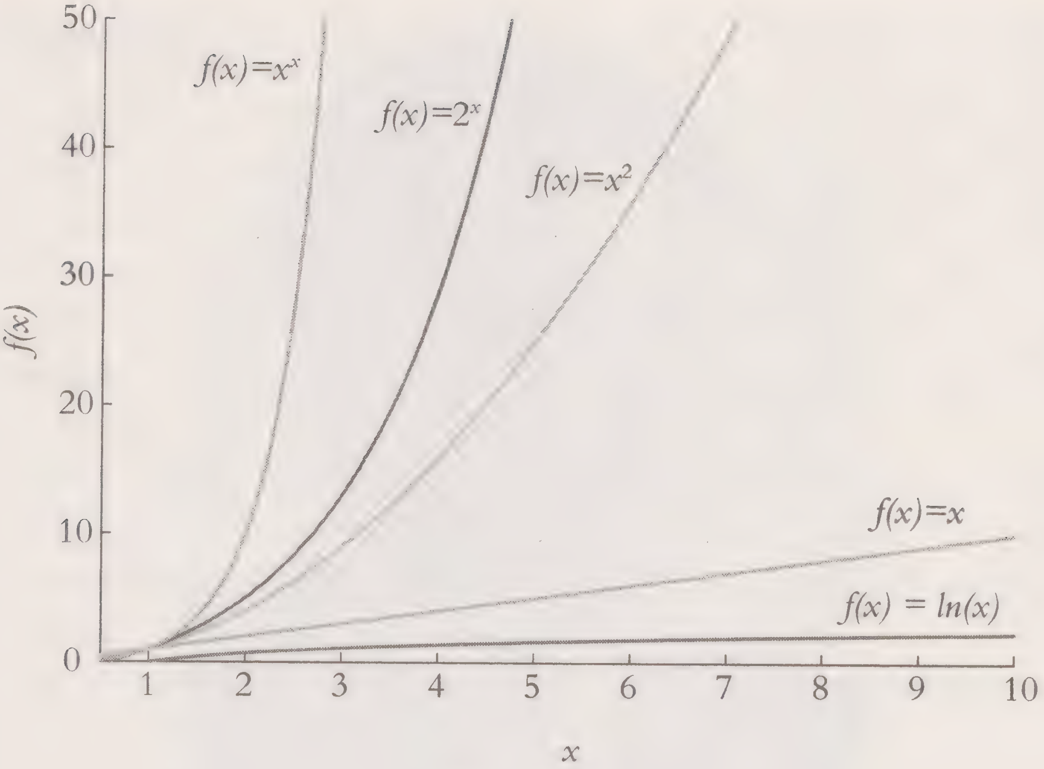
The first preliminary issue to make clear is that from now on, when discussing a problem we will be referring to yes-no decision problems. The question we are faced with is the following: If the answer to a problem is yes, and it is easily checkable, can the problem also be easily solved? That is the thrust of the P versus NP conjecture.

P is the first letter of the adjective *polynomial* and P is the set of problems solvable in polynomial time, in other words in a reasonable, human amount of time; more precisely, a period the duration of which is a polynomial function of the amount of input data. To clarify:

When we're dealing with functions, we know that they 'grow' at a certain rate. Generally speaking, and based on arithmetical inequalities:

$$log\, n \leq n \leq n^a \leq a^n \leq n^n.$$

In general, logarithmic growth is slower than linear growth; the latter is slower than polynomial growth, which in turn is slower than exponential growth; and this in turn is much less steep than hyper-exponential growth. The curves in the following graph show these growth rates.



Growth curves.

If an algorithm runs in polynomial time it simply means that the running time does not grow extravagantly as the initial data grow if the latter are of proportion t. The time it takes is 'of the order' of t^a; it takes no longer than some fixed power of the problem size.

Having defined exactly what the *P* set is, let's move on to *NP*. Now, *NP* does not stand for 'non-polynomial' but rather 'non-deterministic polynomial', which is quite separate and requires a slightly lengthy explanation.

We'll start with a concept that is apparently worlds apart – a 'Turing machine'. Suppose we have a computer with which we can do any type of simple or complex calculation; the calculations will be 'deterministic' in the sense that they will obey our will, our stated intention to calculate something, in a sequential manner, one step after another. The British mathematician Alan Turing (1912–1954) invented a series of mathematical machines, a kind of dream computer, machines that may seem silly and very slow but can perform every imaginable type of calculation. Turing machines are described in a separate box. Computers can be mechanical, electrical, electronic and, in the future perhaps, quantum, but they are all Turing machines. In the eyes of mathematicians, computers don't exist – there are only Turing machines.

So, a problem is a *P*-class decision problem when there is a deterministic Turing machine that can solve the problem in polynomial time.

Alan Turing's life and death sound like something out of a novel. A brilliant mathematician, inventor of the machines that bear his name and hero of World War II for his triumphs as a code-breaker in the legendary Bletchley Park. However, he is said to have committed suicide because he could not cope with society's rejection of his homosexuality.

Now let's look at the difference between deterministic and non-deterministic. A possible solution may be generated by the computer, which is a deterministic machine, but we might also find a solution by chance, or after a laborious individual search involving bouts of insomnia, or in a sudden revelation of mystical origin. There is nothing to say that a solution cannot be found as a result of a non-deterministic procedure. Of course, this solution can be checked, regardless of its origin. That is what we mean when we describe something as non-deterministic.

The *NP* set comprises those problems whose possible solutions – deterministic or otherwise – can be verified with the appropriate information in polynomial time. A problem is *NP* when any potential solution can be checked easily, in polynomial time. For example, a jigsaw puzzle can be *NP*; if it consists of a large number of different pieces it can take a near eternity to solve, but when it has been solved it is a basic task to check that it does indeed tile part of the plane.

THE DREAM CALCULATOR

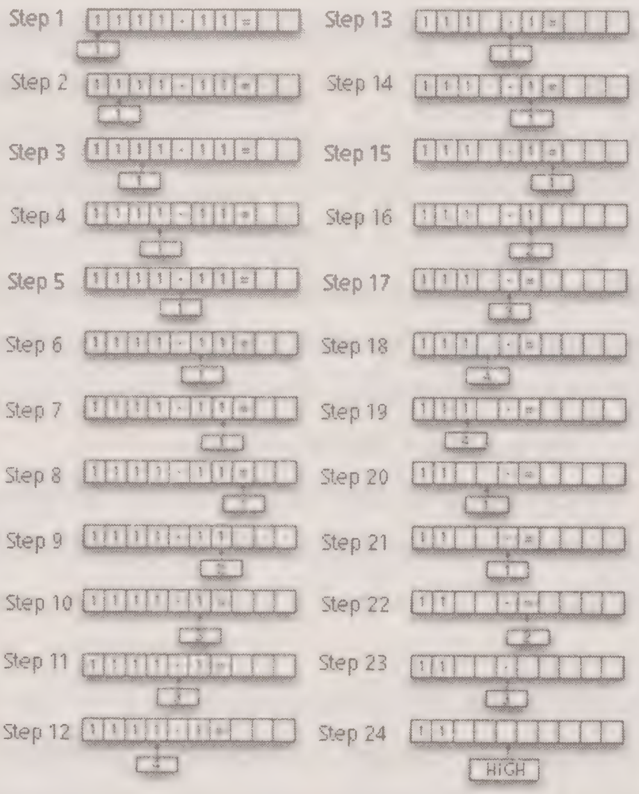
A Turing machine is a kind of mathematical framework for a computer. It consists of tape of infinite length (or not limited in length) marked out into squares, on each of which the initial symbols are written; a reader-writer that reads the tape, writes in the square after reading it and then decides whether to move the tape forwards or backwards and registers the state of the machine; and a finite table that tells us the instruction based on what it reads and the current state of the machine. The machine also keeps a register of the states it is in.

Usually, a Turing machine uses 0s and 1s, but any symbol can be used. It is an imitation of reality that can simulate any calculation, but which in principle could simulate, given the right peripheral elements, any behaviour that any conceivable computer could be capable of.

This is an example of a basic Turing machine which can subtract. Top, the machine table; right, how the machine operates, step-by-step (it just subtracts 2 from 4!).

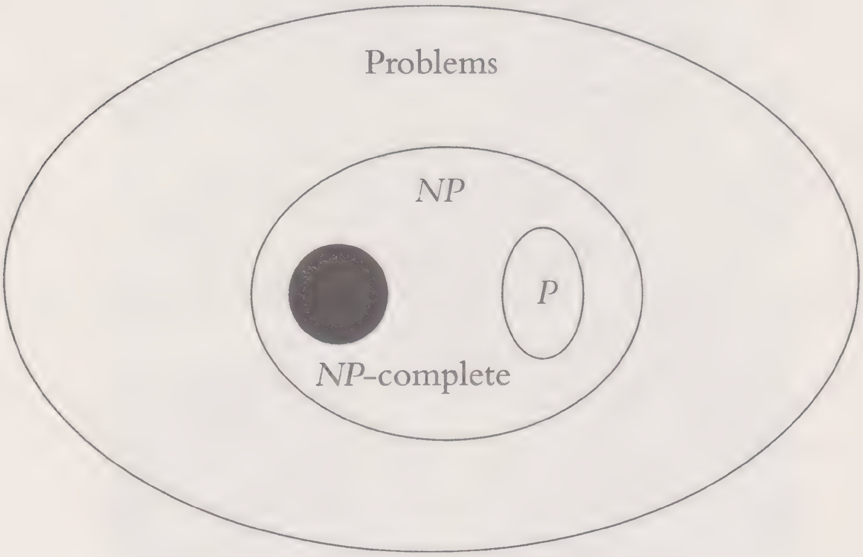
In fact, a Turing machine is a kind of computer without memory problems.

(State, Symbol)	(State, Symbol, Direction)
(1, " ")	(1, " ", forwards)
(1, "1")	(1, "1", forwards)
(1, "−")	(1, "−", forwards)
(1, "=")	(2, " ", backwards)
(2, "1")	(3, "=", backwards)
(2, "−")	(HALT, " ", forwards)
(3, "1")	(3, "1", forwards)
(3, "−")	(4, "−", backwards)
(4, " ")	(4, " ", backwards)
(4, "1")	(1, " ", forwards)


Step 1
Step 2
Step 3
Step 4
Step 5
Step 6
Step 7
Step 8
Step 9
Step 10
Step 11
Step 12
Step 13
Step 14
Step 15
Step 16
Step 17
Step 18
Step 19
Step 20
Step 21
Step 22
Step 23
Step 24
HIGH

Note that $P \subset NP$, because if a problem has a solution in polynomial time, if it is solved it can automatically be checked. The difficulty arises when we ask whether $P = NP$.

As the following is quite complicated, a diagram might be useful.



The set of problems that are non-*P* (which is not the *NP* set; we need to be careful with the terminology) or co-*P* (complement of P) is the set of problems that are not in *P*. Any problems in this set will have solutions, with algorithms that run in non-polynomial time – a huge amount of time. Determining all non-*P* problems is a potentially mind-boggling task. Given a problem, we would have to see all its possible algorithms and check that none is polynomial. *P* would comprise easy problems, so to speak, and to decide whether a problem is non-*P* we would have to demonstrate that it is difficult in every possible circumstance.

Here we will limit ourselves to *NP*, which overlaps partially with non-*P*. After much research, a set of *NP* problems has been compiled which all satisfy the curious criterion that when *one* is solved in polynomial time, the right operation will solve *all* the *NP* problems, also in polynomial time. This subset of *NP* is called *NP*-complete.

Many *NP*-complete problems have been identified (like the well-known game *Minesweeper*), but unfortunately no polynomial time algorithm has been found for any of them. *NP*-complete problems are all *NP-hard,* and we don't know how to begin to solve them. The set of *NP*-complete problems is defined as those *NP-hard* problems that are also in *NP*. In summary, having got this far, we are entitled to ask what the experts think: $P = NP$ *or* $P \neq NP$? The majority opinion is that $P \neq NP$, with 61% in favour and 22% unsure. However, as this poll only asked 100 mathematicians, the answer is not significant.

All of the above may seem to operate on a very high level and have scarcely any impact on the real world, but if we think a little further we'll see that, in essence, we're talking about encryption. Indeed, the security of our credit cards, for instance, is no more than one insignificant example of the more general problem of message encryption.

Imagine that all messages were encrypted using the public key RSA system, the most secure and robust encryption system currently available. Essentially, we're talking about the security of a system that can be boiled down to an *NP* problem: the factorisation of a huge number into two primes, also huge. Anyone who wants to break the code will first have to factorise them. But if we assume that $P = NP$, this would mean that the task of factorising could be completed in polynomial time and that, therefore, there would exist a factorising algorithm that could ultimately run 'quickly', given sufficiently powerful computers.

What use would all our secret messages and encryption be if the keys could be broken using a computer? It makes you shudder to think about it: Big Brother would be just around the corner.

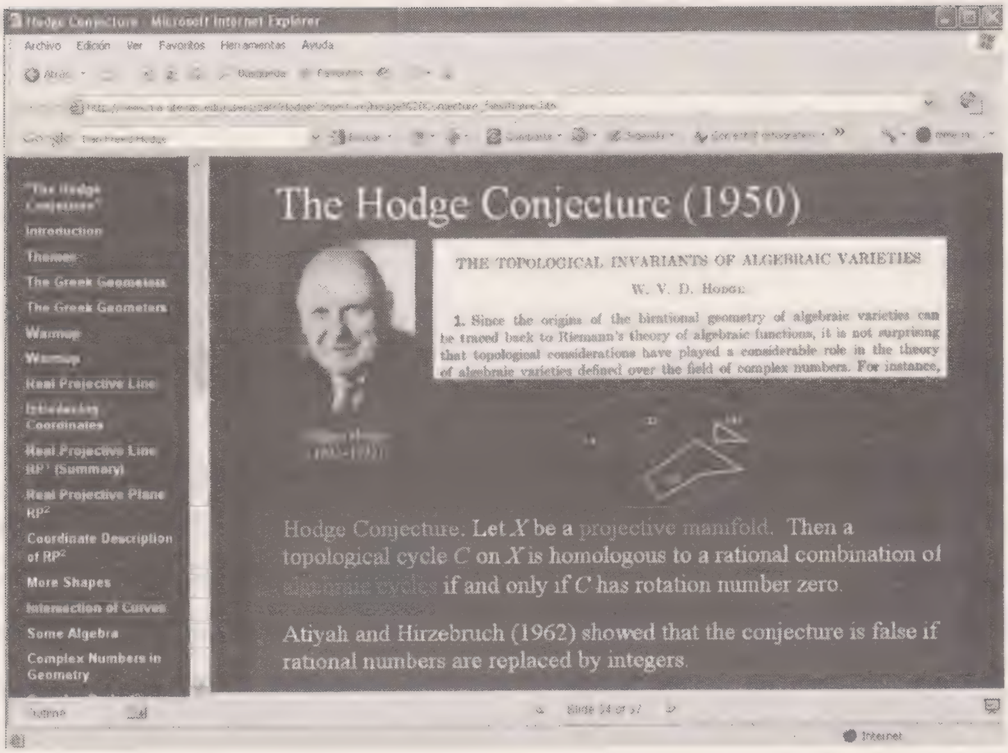
The Hodge conjecture

The second problem on the Clay Institute's list shall remain, like others, concealed by a veil of mystery. Its statement alone is enough to demonstrate why. The problem can be stated as follows:

> Let *A* be a projective complex manifold. Then every Hodge class on *A* is a linear combination with rational coefficients of the cohomology classes of the complex subvarieties of *A*.

Fortunately the Clay problems are widely renowned for being unintelligible and, especially in the United States, there is a tradition of public sessions with videos and slides designed to explain difficult but important concepts to laypeople.

We might find a lecture by an expert in algebraic geometry, like Dan Freed, useful, although we would need to spend several hours on the Internet to follow it.


Hodge Conjecture - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
"The Hodge Conjecture"
Introduction
Themes
The Greek Geometers
The Greek Geometers
Warmup
Warmup
Real Projective Line
Introducing Coordinates
Real Projective Line RP¹ (Summary)
Real Projective Plane RP²
Coordinate Description of RP²
More Shapes
Intersection of Curves
Some Algebra
Complex Numbers in Geometry
Internet

The Hodge Conjecture (1950)

THE TOPOLOGICAL INVARIANTS OF ALGEBRAIC VARIETIES

W. V. D. Hodge

1. Since the origins of the birational geometry of algebraic varieties can be traced back to Riemann's theory of algebraic functions, it is not surprising that topological considerations have played a considerable role in the theory of algebraic varieties defined over the field of complex numbers. For instance,

Hodge Conjecture: Let *X* be a projective manifold. Then a topological cycle *C* on *X* is homologous to a rational combination of algebraic cycles if and only if *C* has rotation number zero.

Atiyah and Hirzebruch (1962) showed that the conjecture is false if rational numbers are replaced by integers.

Dan Freed's web page on the Hodge conjecture.

We can try to make sense of the apparent gibberish of the statement of the conjecture as follows. Geometers have spent years gradually perfecting methods for investigating the shapes of very complicated objects by reducing them to their simplest component parts. This is a useful procedure, but as progress was made, intuition and comprehension gradually fell by the wayside, to the extent that we have now arrived at a point where there is a clear gap between reality and theory. William Vallance Douglas Hodge (1903-1975) helped to simplify the theory somewhat, proposing that a number of structures with component parts, called Hodge classes, are in fact rational linear combinations of simple classes.

The other alternative is to spend years studying mathematics and specialise in algebraic geometry and topology. There we will find objects like simplices, cycles, edges, chains, boundaries, differential forms, and formulae as mysterious and beautiful as these:

$$\int_M d\omega = \oint_{\partial M} \omega$$

$$\cup : H^{p,q}(X) \times H^{p',q'}(X) \rightarrow H^{p+p',q+q'}(X).$$

$$\ldots \leftarrow C^{n+1}(X;G) \xleftarrow{\delta} C^n(X;G) \leftarrow \ldots \leftarrow C^0(X,G) \leftarrow 0.$$

We will also encounter homology and cohomology classes, sheaves, fibre spaces, projective manifolds, subvarieties, the theory of motives and, finally, Hodge classes and his conjecture. With a bit of luck, by the time we have managed to read (and understand) all this, some genius will have come along and solved the conjecture.

The Clay Mathematics Institute itself states: "In the 20th century, mathematicians discovered powerful ways to investigate the shapes of complicated objects. The basic idea is to ask to what extent we can approximate the shape of a given object by gluing together simple geometric building blocks of increasing dimension. This technique turned out to be so useful that it got generalised in many different ways, eventually leading to powerful tools that enabled mathematicians to make great progress in cataloguing the variety of objects they encountered in their investigations.

"Unfortunately, the geometric origins of the procedure became obscured in this generalisation. In some sense it was necessary to add pieces that did not have any geometric interpretation. The Hodge conjecture asserts that for particularly nice types of spaces called projective algebraic varieties, the pieces called Hodge cycles are actually (rational linear) combinations of geometric pieces called algebraic cycles."

If the words of the institute itself are difficult to understand it is because the subject is very difficult to grasp. The introductory description of this problem set out by Pierre Deligne (b. 1944), a distinguished French mathematician who won the Fields Medal in 1977, is also very difficult to follow.

So difficult is the conjecture to formulate correctly that Hodge himself made a mistake in stating it and the *enfant terrible* of the period, Alexandre Grothendieck (b. 1928), published an article in 1969 entitled *Hodge's General Conjecture is False for Trivial Reasons*, revealing the error. A subsequent, more careful restatement cleared up the mess.

A manifold is the term used to describe a surface in algebraic geometry, but to simplify matters the conjecture deals with any dimension. Normally, in n dimensions, k-dimensional manifolds are described by systems of $n - k$ equations defined by n variables. But these manifolds are defined on the basis of real numbers, whereas the Hodge conjecture involves complex numbers. It would be impossible to describe it any further in a way that we as generalists could understand.

The Poincaré conjecture

This is the only Millennium Problem to have been solved so far. In 2002, a Russian mathematician who had already displayed great talent and highly unorthodox behaviour, Grigori Perelman (b. 1966), began to publish a series of papers online which were designed to demonstrate the conjecture. These papers, according to the experts, eventually resolved all the unknowns raised. It's useful to know that there is a website *arXiv* where researchers can post their 'raw' results, without going through the sometimes very lengthy – but ultimately essential – process of scrutiny by the experts on the question, who will detect any mistakes. But it appears there weren't any errors in Perelman's submissions.

In 2010, after clearing all the hurdles erected by the cautious statutes of the Clay Mathematics Institute, Perelman was awarded the $1,000,000 prize. The preconditions were satisfied, and the Poincaré conjecture is now the Poincaré theorem.

To begin with, we should note that Henri Poincaré (1854–1912) was an exceptional mathematician, the leading mathematician of his time. The Poincaré conjecture – henceforth theorem – stated in 1904, goes as follows:

> "Every simply connected, closed three-dimensional manifold is homeomorphic to the 3-dimensional sphere."

MATHEMATICIANS IN THEIR WORLD

Grigori Perelman.

At the 2006 meeting of the International Union of Mathematicians in Madrid, Grigori Perelman was awarded the Fields Medal, the highest honour for a professional under the age of 40 who has made an outstanding achievement to mathematics. Perelman declined the award. As reported in the *Daily Telegraph*, Perelman was not the first person to turn down an honour; in other fields, Jean-Paul Sartre and Marlon Brando did it voluntarily and Boris Pasternak was forced to do it. But this indifference to material goods was surprising from somebody who lives with his elderly mother in a modest apartment in Saint Petersburg. But he was not the first mathematician to display an extravagant disregard for the world and its trappings. The exceptionally gifted genius of pure mathematics, Alexandre Grothendieck (b. 1928), who is stateless, turned his back on his science at the age of 62 and apparently now leads a semi-hermetic existence in a remote part of southern France. As Du Sautoy says, "you have to be a bit mad to be a mathematician". He might have a point.

Part of a photograph taken during the 1911 Solvay Conference. Poincaré is in the front row, seated first from the right, next to Marie Curie. In the back row, standing second from the right, is Albert Einstein.

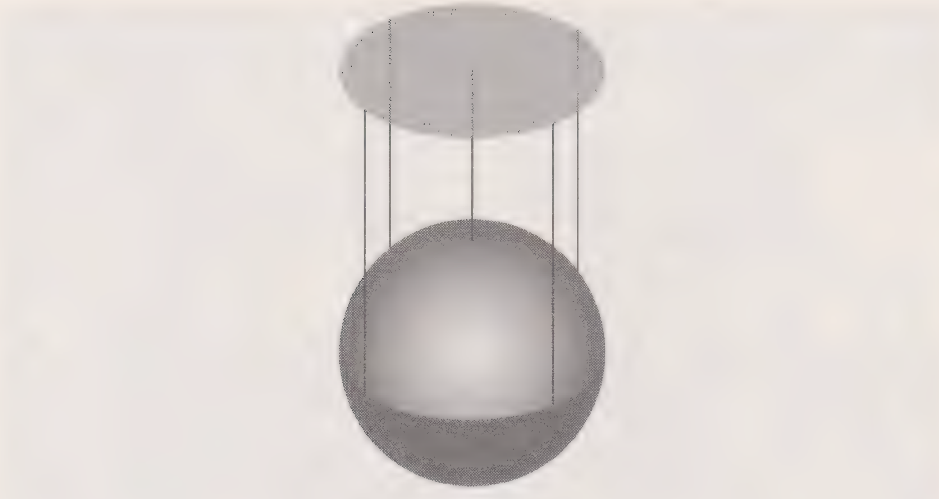
Let's take one thing at a time. This fairly intimidating statement is in fact quite easy to explain. An n-dimensional manifold is an algebraic object defined by an equation with $n + 1$ unknowns; when the manifold is differentiable, it has a smooth (closed) surface, with no cusps or strange edges. In one dimension, a sphere of radius r, for example, is a manifold called a circle and is defined as the set of points S^1 which satisfy:

$$x_1^2 + x_2^2 = r^2.$$

Similarly, a sphere of radius r is the manifold:

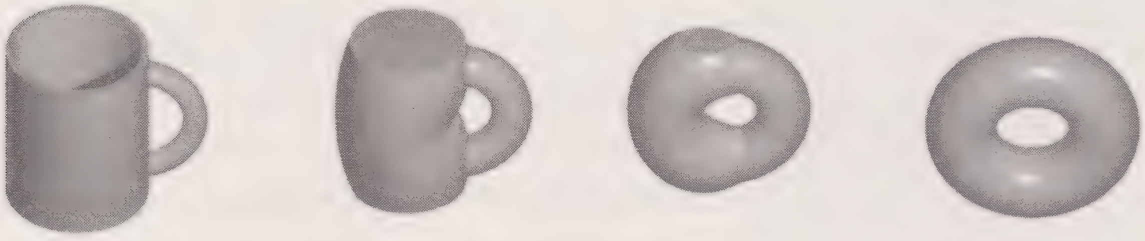
$$x_1^2 + x_2^2 + x_3^2 = r^2,$$

and shares with other manifolds in Euclidean space the following characteristic – it can be deformed into simpler pieces and rebuilt.



Two circles, when continuously deformed and rebuilt, can form a two-dimensional sphere.

A homeomorphism, in the field of topology, is any continuous transformation that retains its form. For instance, a coffee cup and a doughnut are homeomorphs, because one can be changed into the other in a continuous, unbroken transformation. Conversely, a coffee cup and a ball are not, because however much a cup is continuously deformed, it will always have a hole (or handle), which cannot be transformed into a ball.



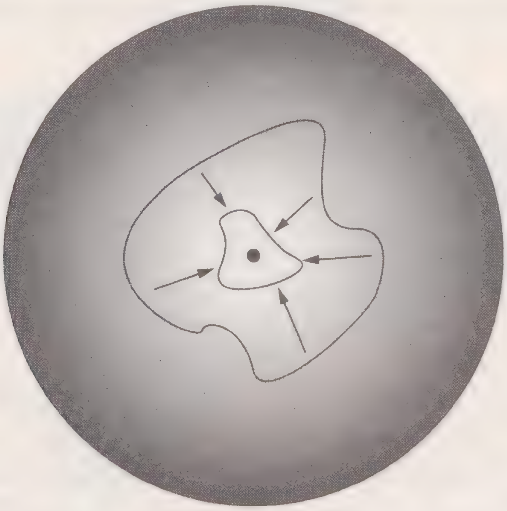
On the other hand, a ball is homeomorphic to a cube or any other compact object without holes – even the monolith in *2001, A Space Odyssey.* Not all homeomorphisms are as straightforward, but this gives us an idea of the subject.

Compactness means, in fact, that the manifold is not unlimited, but rather a closed surface. In $\mathbb{R}^n$, compact means closed and delimited.

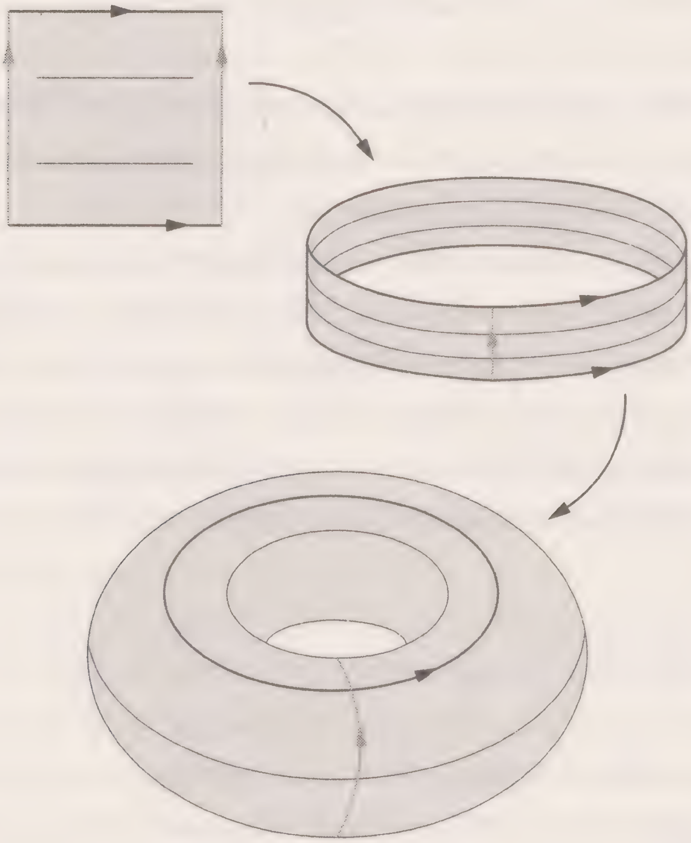
The term 'closed' in the statement is very simple to explain. This criterion rules out manifolds with cusps or strange edges. The rounded forms of an ellipsoid, for example, are permitted.

A shape, informally speaking, is simply connected when it has no holes. And more formally, a surface is simply connected when given a point P, any loop (closed curve) on the surface which passes through P can be contracted to a point, or in other words, when any loop on the surface is homeomorphic to a point.

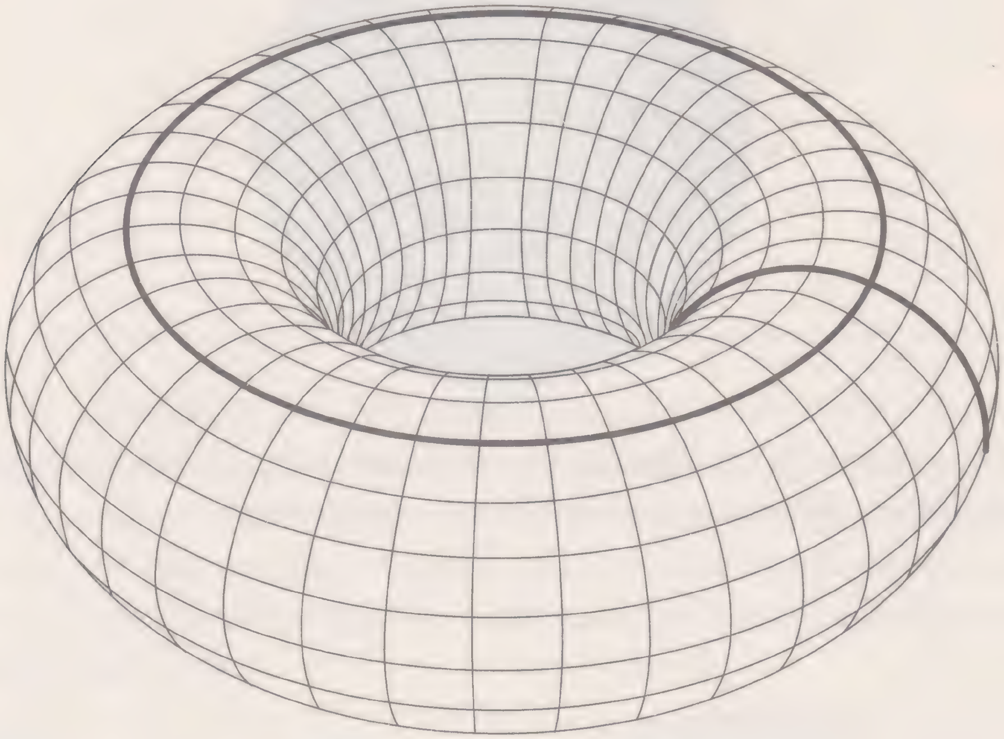
The torus and the sphere are often used to demonstrate simply connected surfaces. If a loop is drawn around a sphere it can be contracted to a point.



A torus or toroid is a (hollow) doughnut-shaped surface that can be formed by taking a cylinder and joining the two circular edges together.



If two loops are drawn, as in the diagram on this page, they cannot be contracted to a point over the surface of the torus. The surface itself prevents it, as the loop cannot go through the torus – it would have to cut through it.



In terms of homotopy, which is the topological theory deriving from grouping closed curves together, S^2 has a trivial homotopy group, reduced to a single member, while a torus has a non-trivial homotopy.

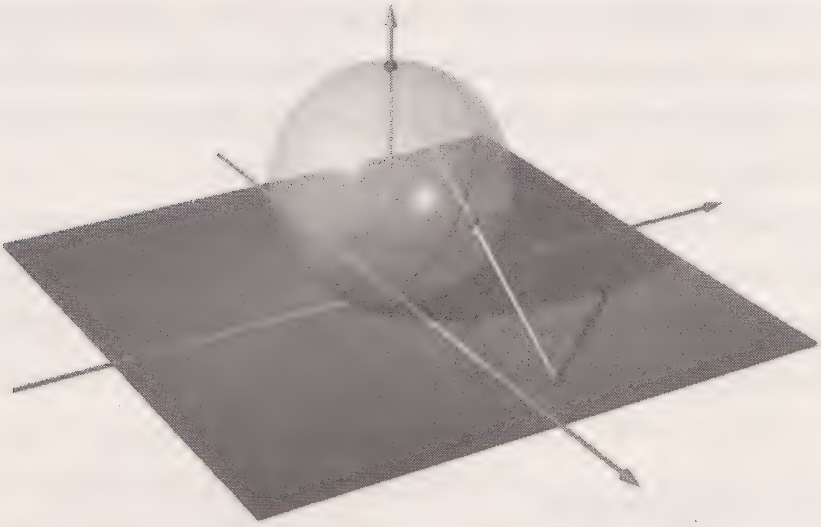
The Poincaré conjecture states, in short, that in three dimensions, the only 'normal' simply connected surface is the sphere S^3. This had been established in the other dimensions. What was missing, and took nearly a century, was proof for the sphere in three dimensions. Be careful though, because a 3-sphere (three-dimensional) is a hypersurface, which is difficult for us to comprehend straight away.

It might be helpful to understand what a sphere is. A sphere is defined in terms of $\mathbb{R}^n$ as:

$$S^n = \{x \mid x = (x_0, \ldots, x_i, \ldots, x_n) \ y \ x_0^2 + \ldots + x_i^2 + \ldots + x_n^2 = r^2\}$$

in other words, as a ball of radius *r*.

In two dimensions it is clear that the sphere is equivalent to a plane plus a 'point at infinity'.



The so-called stereographic projection is a smooth, bijective mapping of S^2 onto the plane. Only one point on the sphere, its north pole, is not paired off in this mapping. The situation is rescued by designating this point the 'point at infinity' of the plane, which 'compresses' the sphere and makes it a compact set. The procedure operates in the same way for a circle.

In higher dimensions similar operations can be carried out. In fact, a similar equivalence was used by Stephen Smale (b. 1930), a mathematician with a fairly original *Weltanschauung* (world view), to prove the Poincaré 'theorem' for dimensions n $\geqq$ 5, in 1960. Michael Freedman did the same but with greater difficulty for dimension 4 in 1982. In 1986 he too was awarded the Fields Medal.

The only unproven dimension was $n = 3$, and this remained the case for many years. In the 1970s Fields medallist William Thurston (b. 1946), regarded as an infuriatingly meticulous researcher but a brilliant mathematician, established geometric criteria in the form of a conjecture which, if proven, would have seen off the Poincaré conjecture. Unfortunately, as happens so often for this type of conjecture, there was no way of proving it. Thurston found eight geometric structures and conjectured that 3-manifolds could be classified on the basis of these structures. The Poincaré conjecture was deduced from this classification.

Into the story stepped Richard Hamilton (b. 1943), an American mathematician who proposed a strategy for attacking the problem based on a concept with physical connotations that he himself had discovered – the Ricci flow. This deforms the metric of a Riemannian manifold in much the same way as the diffusion of heat.

Perelman followed the path marked out by Hamilton in his reasoning. In fact he refined it, using concepts with such colourful names as 'Ricci flow with surgery'.

And they sound fun because they are, to mere mortals, as incomprehensible and inaccessible as the music of the spheres. He ultimately demonstrated an even more general result than Thurston's geometrisation and, therefore, the Poincaré conjecture, which follows from it.

So indebted did Perelman feel to Hamilton that he turned down the prize for solving a Millennium Problem, arguing – among other things – that Hamilton deserved the award too. So there was no clear winner of the first million dollars, or at least it did not end up in Perelman's pocket.

The Riemann hypothesis

We now come to what the experts regard as the most important unresolved problem in mathematics. It has even starred on the silver screen. In *A Beautiful Mind* the main character, Nobel laureate John Nash, sees his efforts to prove the question thwarted by the drugs he is taking for his schizophrenia. The widely revered Charles de la Vallée Poussin said that whoever solved the Riemann hypothesis would cover himself in glory. Enrico Bombieri, Fields medallist and recognised expert on the subject, thinks that the fall of the hypothesis will wreak havoc in the field of prime number distribution. Others, like Peter Sarnak, who wrote the official description of the problem for the Clay Institute, have predicted that the world will be a very different place if the hypothesis is disproved.

A MATHEMATICIAN WITH A SENSE OF HUMOUR

The Riemann hypothesis is so important that it has provoked the strangest behaviour in the most balanced individuals. Mathematician Godfrey Harold Hardy once had to catch a boat from Scandinavia to the UK while a storm raged in the tempestuous North Sea. He sent a postcard to his friend Harald Bohr. "I've solved the Riemann hypothesis" was the message. Luckily Hardy arrived without mishap at his destination and then sent Harald a correction denying the achievement. The news did not make the newspapers. Hardy, whether with good humour or sound logic, gave this rationale for his postcard: God, in His infinite wisdom, was certainly not going to allow an atheist mathematician to go to his grave with a secret like that; the boat had to reach port safely or a non-believer would go down in history with a romantic aura attached to him that only He, God, would know was unmerited.

While there is a cash prize available, demonstrating the Riemann hypothesis is worth more than just a million dollars. It is worth much more in prestige, admiration, conferences, envious looks, front pages in daily newspapers, etc. What is indisputable is that it has been waiting a century and a half for a response that has so far not come. Some serious and acclaimed experts, such as the Argentine-American Gregory John Chaitin (b. 1947), have expressed doubts as to whether a proof will ever be forthcoming. Will the Riemann hypothesis be an undecidable question? Gödel proved the existence of such statements. In logical systems of a certain structure, particularly those that include elementary arithmetic, there are always consistent statements that cannot be proved using the rules of the system. It is a curious situation indeed when a legitimate mathematical statement can exist like "it can be demonstrated that something can never be demonstrated".

There is nothing to suggest that the Riemann hypothesis will be unprovable; indeed it has already been endorsed – but never proved – by trillions of individual cases which seem to reinforce it. It has actually been proved in finite fields by Deligne. Until recently attempts were being made to attack it via quantum mechanics. But a small lingering worry still remains: what if the Riemann hypothesis is one of those problems of unimaginable, exponential computational complexity?

Let's move on to the famous hypothesis, the statement of which is fairly innocuous and perhaps even a little disappointing, because at first glance it seems immaterial. Consider the complex function ζ (we will refer to it using the Greek letter zeta), i.e. defined in the field ℂ of complex numbers with a real part greater than 1.

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\dots \quad \Re(s)>1.$$

In the 17th century, Euler used it to pull off one of his usual immense algebraic juggling acts. He identified it with the infinite product which extends, as if by magic, over all prime numbers. This is an early hint of the use Riemann intended to make of it.

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_{p\text{ prime}}\frac{1}{1-p^{-s}}.$$

Euler's transformation worked as follows:

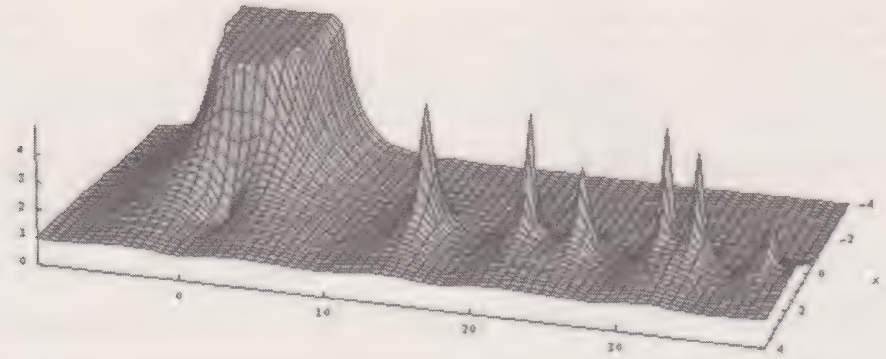
$$\prod_{k=1}^{\infty}\frac{1}{1-\frac{1}{p_k^s}}=\frac{1}{1-\frac{1}{p_1^s}}\frac{1}{1-\frac{1}{p_2^s}}\frac{1}{1-\frac{1}{p_3^s}}\dots=\left[\sum_{k=0}^{\infty}\left(\frac{1}{p_1^s}\right)^k\right]\left[\sum_{k=0}^{\infty}\left(\frac{1}{p_2^s}\right)^k\right]\left[\sum_{k=0}^{\infty}\left(\frac{1}{p_3^s}\right)^k\right]\dots=$$

$$=\left(1+\frac{1}{p_1^s}+\frac{1}{p_1^{2s}}+\frac{1}{p_1^{3s}}+\dots\right)\left(1+\frac{1}{p_2^s}+\frac{1}{p_2^{2s}}+\frac{1}{p_2^{3s}}+\dots\right)\dots=$$

$$=1+\sum_{1\le i}\frac{1}{p_i^s}+\sum_{1\le i\le j}\frac{1}{p_i^s p_j^s}+\sum_{1\le i\le j\le k}\frac{1}{p_i^s p_j^s p_k^s}+\dots=1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\dots=\sum_{n=1}^{\infty}\frac{1}{n^s}=\zeta(s).$$

For those familiar with complex analysis, in the standard procedure the zeta function can be extended as a meromorphic function to the whole complex plane with a single pole $s = 1$, where the residue is 1. This is the ζ function that Riemann was referring to in his hypothesis.

The zeta function, as it is complex and has a complex variable, requires four parameters and, therefore, four Cartesian axes to represent it correctly. In other words, it cannot be represented graphically. If we restrict ourselves to three axes and plot on the vertical axis the modulus of the complex input number, $|\zeta(z)|$, which is a real number instead of the complex value $\zeta(z)$, we get a graph like the one below.

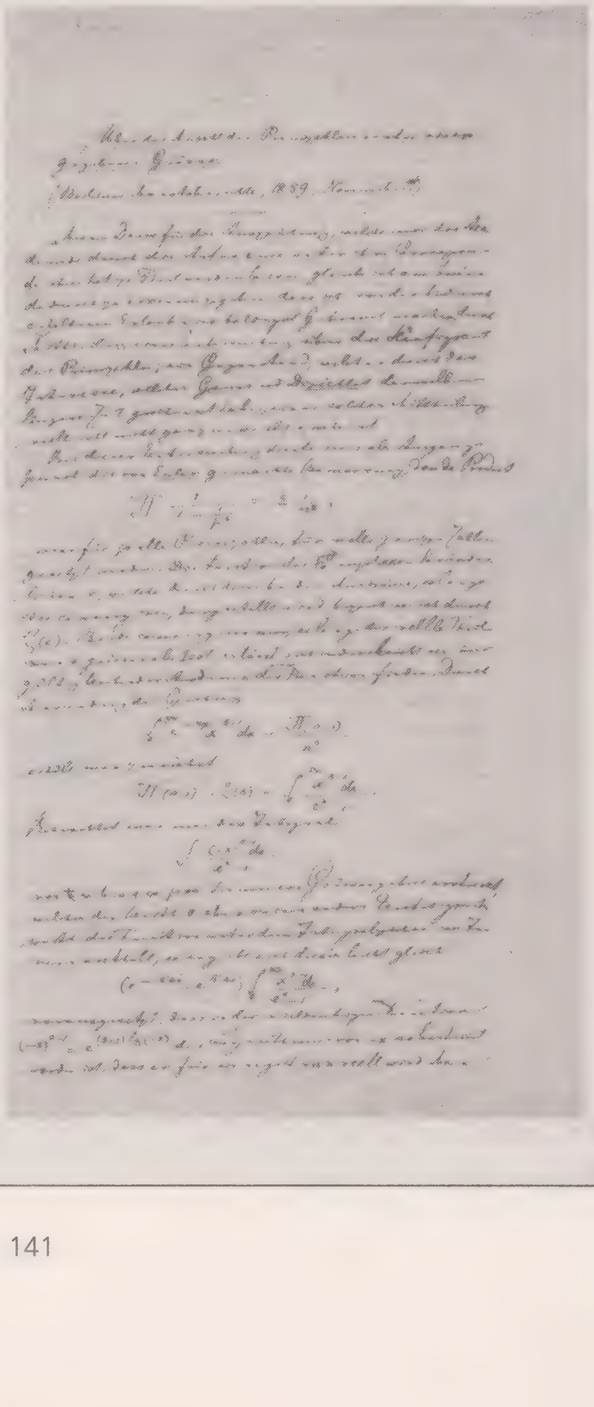


In zeta we are interested in the zeros, the points at which it vanishes. At negative even real numbers, zeta vanishes. These are called trivial zeros. We are interested in the non-trivial zeros. So, the Riemann hypothesis states that: "All non-trivial zeros of the ζ (z) function lie on the straight line with real part 1/2."

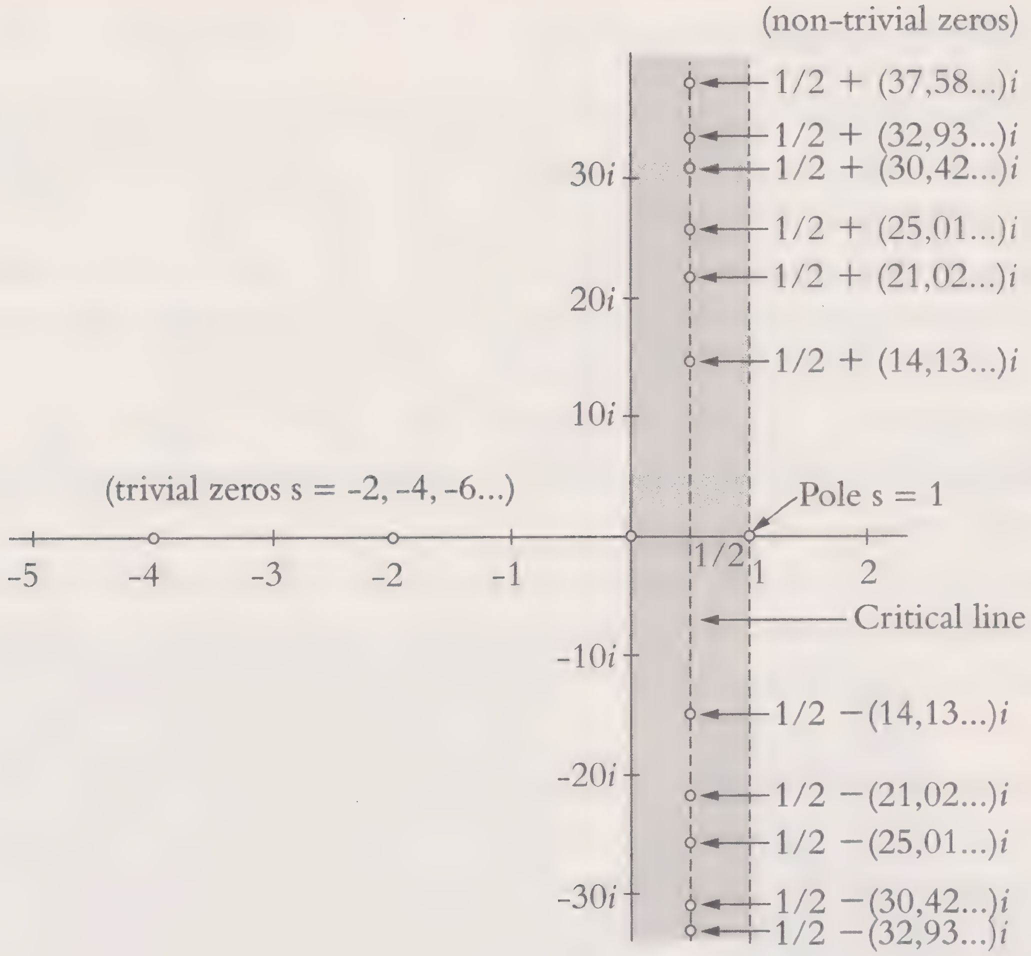
In a less visual but more informative form, the Riemann hypothesis asserts that the non-trivial zeros lie within the critical zone, specifically along the vertical line $\Re(z) = 1/2$.

BERNHARD RIEMANN (1826–1866)

This notable mathematician was the first to use the ζ function in his paper *Über die Anzahl der Primzahlen unter einer gegenbenen Grösse* (*On the Number of Primes Less Than a Given Magnitude*), published in November 1859. Riemann was already a mathematician of global renown and formidable stature, respected and admired by all, including the veteran Gauss, who taught him at university and supervised his doctoral thesis. Riemann died of tuberculosis, a scourge of his time, and as in the case of other genii who died young, we can only ask ourselves what more he might have achieved. He made his mark in every field he worked in, although geometric spaces of variable curvature and prime numbers are those in which his name comes up most often.



Portrait of the German mathematician Riemann and copy of one of his manuscripts, kept at the University of Göttingen. In this work, which only contains six pages, he states the famous Riemann hypothesis. Formulated for the first time in 1859, one and a half centuries later this hypothesis is still regarded as one of the most important unsolved problems in modern mathematics.


(non-trivial zeros)
1/2 + (37,58...)i
1/2 + (32,93...)i
1/2 + (30,42...)i
1/2 + (25,01...)i
1/2 + (21,02...)i
1/2 + (14,13...)i
30i
20i
10i
(trivial zeros s = -2, -4, -6...)
Pole s = 1
-5
-4
-3
-2
-1
1/2
1
2
Critical line
-10i
-20i
-30i
1/2 −(14,13...)i
1/2 −(21,02...)i
1/2 −(25,01...)i
1/2 −(30,42...)i
1/2 −(32,93...)i

What do the zeros of a complex function have to do with prime numbers? We will not provide a detailed explanation here – it would be very long and difficult to follow – but we will sketch an outline. The Riemann $R(x)$ function has already made a fleeting appearance, when we were discussing the prime number theorem. Its link to the ζ function becomes clear after a number of calculations:

$$R(n)=1+\sum_{k=1}^{\infty}\frac{1}{k\,\zeta(k+1)}\frac{(\log n)^k}{k!}.$$

The R function was introduced by Riemann himself and is usually defined by:

$$R(n)=\sum_{n=1}^{\infty}\frac{\mu(n)}{n}Li(x^{1/n}),$$

where $\mu(n)$ is a rather elaborate way of saying 0, +1 or −1. It is called the Möbius function and $\mu(n)$ equals:

- 0 if n has one or more repeated prime factors.
- $+1$ if $n = 1$.
- $(-1)^i$ if n is the product of i different prime numbers.

Remember that:

$$Li(x)=\int_2^x \frac{du}{\log u}.$$

The function $R(x)$ is an 'improvement', a refinement of $Li(x)$ introduced by Riemann for probabilistic reasons. Moving on to questions in the field of functional calculus it is clear that $R(x)$ has significant links to the zeta function, and it is also clear how knowledge of the zeros of $\zeta(x)$ offers a much greater insight into the oscillations of $R(x)$ around $\pi(x)$, the ideal function, the long-sought function defined by:

$$\pi(x) = \text{number of prime numbers less than } x.$$

The following table shows the excellent approximation provided by $R(x)$:

	$\pi(x)$	$R(n)$
100,000,000	5,761,455	5,761,552
200,000,000	11,078,937	11,079,090
300,000,000	16,252,325	16,252,355
400,000,000	21,336,326	21,336,185
500,000,000	26,355,867	26,355,517
600,000,000	31,324,703	31,324,622
700,000,000	36,252,931	36,252,719
800,000,000	41,146,179	41,146,248
900,000,000	46,009,215	46,009,949

This all leads us to believe that if the hypothesis is proven, the road to the calculation of these oscillations of $R(x)$ will be virtually clear, and that our path to knowledge of prime numbers will open up in front of us like the waters of the Red Sea before Moses and his people. But for the moment, while the number theorists wait with baited breath, the waters refuse to part and the promised land is not yet in sight.

In the meantime, we have found dozens of propositions equivalent to the Riemann hypothesis. One states:

$$\left|\pi(x) - Li(x)\right| < \frac{1}{8\pi}\sqrt{x}\ \log x \text{ while } x > 2656.$$

Another, which we quote for its brevity and beauty, is:

$$\sigma(n) < e^{\gamma} n \log \log n \text{ for any } n > 5{,}040,$$

where $\sigma(n)$ is our old friend the 'divisor function' we defined when we were discussing perfect numbers, and γ the Euler-Mascheroni constant. And many more, some from such apparently remote fields as group theory.

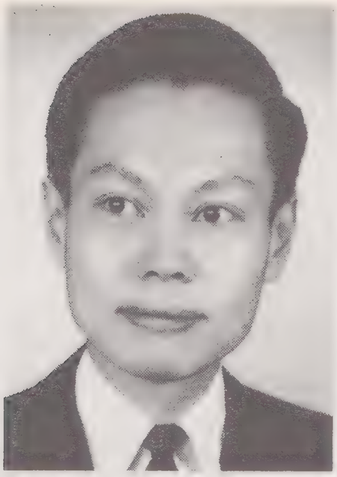
There are also stronger conjectures than the simple Riemann hypothesis; if the former were proven, the latter would inevitably follow. But we won't go into them here because we have set out the basics. The bottom line is that this is a conjecture which, in the more than ten billion cases scrutinised so far ('ten trillion' in the USA), has never been disproved.

The green fields of Yang-Mills

In the micro-world of the very, very small, the only things that come in a variety of colours (and even flavours) are quarks governed by quantum chromodynamics which, we know, contains colour quantum numbers (there are six quarks with different *flavours*, each one allowing three *colours*). The Yang-Mills theory belongs to field theory, and concerns a type of field, a generalisation of quantum electrodynamics and the single electromagnetic field conceived by John Clerk Maxwell (1831–1879) many years ago. His equations, the so-called Maxwell equations, dominated physics for a long time.

Before getting into more detail, we will note that Robert Mills (1927–1999) was an American physicist who worked happily for 39 years at the same university (Ohio), and in 1954 revealed, alongside his colleague Chen Ning Yang (b. 1922), a new and broad field concept, which bears his name.

In quantum physics, forces act in a circular manner around a field. In addition, the components are governed by a symmetry group, which is the *gauge* group of the field. In fact, a meticulous mathematical definition would lead us to posit the invariance of the Lagrangian of the field on which the gauge group acts, but we are already into

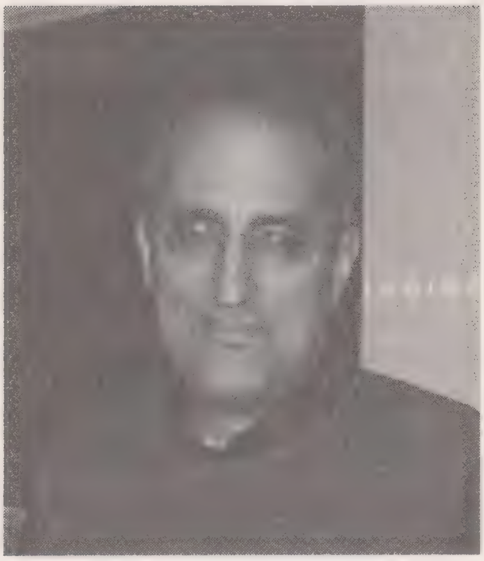


Of the Yang-Mills duo, the most outstanding researcher is Chen Ning Yang (pictured), who in 1957 received the Nobel Prize for Physics for his discovery of parity non-conservation.

very counter-intuitive territory. In electromagnetism, the gauge group is the $U(1)$ Lie group. In quantum chromodynamics, the gauge group is $SU(3)$. In what we now call the standard model of quantum physics, the group is $SU(3) \times SU(2) \times U(1)$ and the result is a theory that provides a fairly good unified explanation of electromagnetic forces, weak interaction and strong interaction. However, the mathematical aspects of fields and gauge groups are not generally well known and for the time being it seems that little progress can be made in this area.

The Clay Institute focuses on fields and, in particular, the official description of the problem, by the brilliant Edward Witten (b. 1951), asks various questions. Firstly, it asks for a construction of the Yang-Mills fields which is valid for all compact simple gauge groups. In addition, the said construction should take account of a documented phenomenon, quark confinement, which explains why it is impossible to see them individually. In other words, the theory should explain why we live in a universe that is not inundated by quarks.

The theory should also explain the phenomenon of *mass gap*, the absence of mass; while an attempted explanation of this may be somewhat muddled without a reference to higher concepts, we can say that particles, which behave very demurely when in a vacuum and immobile, behave very differently in the presence of energy. When they move they must be assigned a mass ($E = mc^2$ is the famous equivalence formula) which is consistent with levels of excitation. The mass gap arises between level zero and the first energy level, and the proposed theory must explain this in order to accommodate strong forces and explain their short range. There cannot be arbitrarily small levels of excitation.



Edward Witten is the only Fields medallist (1990) not to be a professional mathematician. Instead he is a physicist who has made incredibly important contributions to quantum physics and string theory. His brother Matt, however, a producer and scriptwriter of famous television series such as House M.D.*, is probably more famous than he is.*

Unsolvable equations

While the previous problem is a physics problem, it seems very modern. This is to be expected, because its statement borrows from the cryptic field that is quantum physics, the discipline that, to paraphrase Arthur C. Clarke, is to most laypeople indistinguishable from witchcraft. In the quantum world, it is impossible to know everything about a particle because when we think we've located it, we then don't know how it moves. Solid particles cross impenetrable walls (but we never know whether or not a particular particle will do so). Particles separated by unimaginable distances instantly 'remember' their past and behave as if they were joined... It is a world that obeys only its laws, which are probabilistic and uncertain when considered individually, and inexorable if considered as a whole.

The next Millennium problem is also a physics problem, but it does not belong to the modern branch. It is more a question of Newtonian physics. The Navier-Stokes equations govern the macroscopic and tangible world of fluid dynamics, the science of fluids in motion, and its dictates are universally accessible. Precise weather forecasting is governed by these intractable equations. Unfortunately, there is no way of knowing what they dictate, as there is no way of solving the equations.

Claude-Louis Navier (1785–1836) was a brilliant French physicist and engineer, a specialist in bridge building, like Stokes, who succeeded Cauchy when the latter retired from his professorship. He owes his fame to the formulation of the famous fluid dynamics equations, which bear his name and that of Sir George Gabriel Stokes (1819–1903).

Sir George Gabriel Stokes outdid even Newton's record, being simultaneously a member of parliament, Lucasian Professor in the University of Cambridge and President of the Royal Society.

The famous equations, expressed in vector language for brevity, can be stated as follows:

$$\frac{\partial \mathbf{v}}{\partial t} + (\mathbf{v} \cdot \nabla)\mathbf{v} = -\nabla p + \nu \Delta \mathbf{v} + \boldsymbol{f}(\boldsymbol{x}, t)$$

$$\nabla \cdot \mathbf{v} = 0.$$

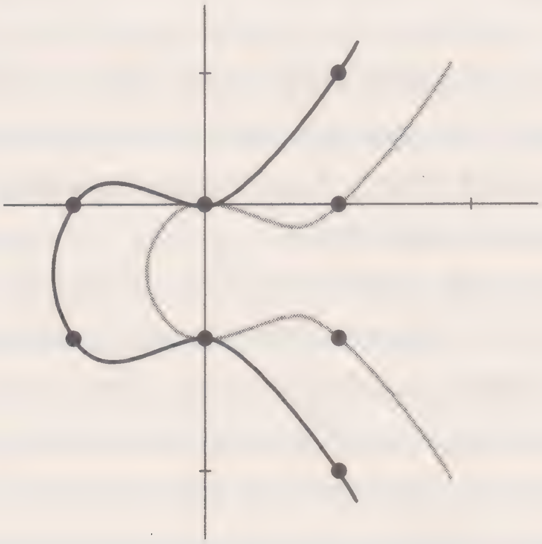
The many deltas (Δ) and nablas (∇) represent, respectively, the Laplacian and the gradient, two operators in the field of partial derivatives. Here **v** is the velocity of the particle, located at $\boldsymbol{x}$ and subjected at the time t to a force $\boldsymbol{f}$. The viscosity of the fluid is $\nu > 0$ and p denotes pressure.

The vector script does not obscure the fact that the equations may be planar (two-dimensional) or spatial (three-dimensional), leaving time aside. They are very attractive expressions, but have so far remained unsolvable. They contain non-linear partial derivatives, and it is unknown whether solutions exist, or at least mathematically exact and deducible solutions, because there are approximate solutions for any type of initial conditions, and computers have been set to work on them. Numerical computer-generated approximations are improving all the time, to the extent that in many cases huge, cumbersome wind tunnels are now being replaced by fully digital equivalents, which take up much less space. But they are just approximations, since turbulence develops immediately and relatively little is known about the equations, except the odd assertion that at quasi-rest nothing seems to happen.

In two dimensions, the Russian mathematician Olga Ladyzhenskaya (1922-2004) solved the problem in the 1960s, and the malevolent *maelstroms* or vortices that wrecked Captain Nemo's *Nautilus* in the final chapter of *20,000 Leagues Under the Sea* are not acceptable in two dimensions, at least spontaneously. The three-dimensional case, meanwhile, remains unsolved.

The mother of all conjectures

Why are we referring to the last of the Millennium Problems like this? For one simple reason: its complete unintelligibility to the layperson (and to non-experts in algebraic geometry and number theory in particular). Perhaps a few preliminary words will help. For many years, algebraists have been interested in Diophantine equations (equations in the field $\mathbb{Q}$ of rational numbers). Indeed Hilbert's tenth problem focuses on this area. And although it was proved by Yuri Matiyasevich that, generally speaking, there is no algorithm for determining when such equations have a solution, this is not the reason why the situation is so complicated. There are some equations that can be solved and the Birch-Swinnerton-Dyer conjecture, if proven, would help us to assess the number of these equations. But remember, if the conjecture is proven, it will not give us a procedure or an algorithm; rather, it will tell us how many solutions there are, and there are a lot.



Two curves, $y^2 + y = x^3 - x^2$ (in grey) and $y^2 + y = x^3 + x^2$ (in black): if we look for their rational points, they become Diophantine equations. They are so similar that it is surprising to learn that the grey curve has four solutions, while the black one has infinite solutions. If we had considered the circumferences $x^2 + y^2 = 1$ and $x^2 + y^2 = 3$, we would have been staggered. The former has infinite rational solutions and the latter, none!

In addition, the highly complicated statement of the conjecture looks like the archetypal rabbit-out-of-a-hat. Experts who manage to understand it will rub their eyes in disbelief. How can such an elaborate function L codify such valuable information on a curve E, seeing as conceptually the objects are worlds apart?

The conjecture can be stated as follows. Let E be an elliptic curve over $\mathbb{Q}$ whose associated L-function we will denote by $L(E,s)$. Then

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^R}=\frac{|Sha|\cdot\Omega\cdot Reg(E/\mathbb{Q})\cdot\prod_p C_p}{|E_{tors}(\mathbb{Q})|^2}.$$

In this formula:

- R is the rank of $E/\mathbb{Q}$.
- Ω is either the real period, or double it, of the minimal model of E. It depends on whether $E(\mathbb{R})$ is connected or not.
- $|Sha|$ is the order of the Tate-Shafarevich group of $E/\mathbb{Q}$.
- $Reg\ (E/\mathbb{Q})$ is the elliptic regulator of $E/\mathbb{Q}$.
- $|E_{tors}(\mathbb{Q})|$ is the number of torsion points on $E/\mathbb{Q}$ (including the point at infinity).
- c_p is a local elementary factor, equal to the cardinality of $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$, where $E_0(\mathbb{Q}_p)$ is the set of points on $E(\mathbb{Q}_p)$ whose reduced modulo p is non-singular at $E(\mathbb{Q}_p)$.

The associated L-function is an infinite product, very similar to the zeta function, which is written

$$L(E,s)=\frac{1}{(1-\lambda^s)}\prod_{p\neq\lambda}\frac{1}{(1-a_p p^s+p^{1-2s})},$$

wherein a number of elements need to be defined: λ is the *conductor*, a special number that depends on each curve; $a_p = p - N_p$, which in turn obliges us to define N_p. This is something like the number of solutions (all rational, belonging to the field $\mathbb{Q}$) when we consider the modulo equation p.

The L-function allows a Taylor series development, and the conjecture therefore allows a slightly less aggressive formulation:

"The Taylor series development at the point $s = 1$ is of the form:

$$L(C,s) = c(s - 1)^r + \text{higher order terms},$$

with $c \neq 0$ and $r = \text{ran}\ (C(\mathbb{Q}))$."

Let's finish with a word on the protagonists of this problem. Bryan Birch (b. 1931) is a notable British mathematician and member of the Royal Society, and Sir Peter Swinnerton-Dyer (b. 1927) is an aristocrat and mathematician, member of the Royal Society and international bridge player. It is no surprise that the description of the Birch-Swinnerton-Dyer conjecture was written for the Clay Institute by someone with the profile of Sir Andrew Wiles, because the conjecture belongs to exactly the same field as the better Fermat theorem. Nonetheless, if it is proven, it is unlikely that it will hit the headlines, because it's hard to imagine a journalist winning a Pulitzer Prize for something so baffling. And, for that matter, so difficult.

Epilogue

Varied are the languages and varied the people.
And a single love will go by many names.
Salvador Espriu

Mathematical problems are a little like the languages Espriu was referring to: they are innumerable, but they are indispensable. They are the drivers of our most abstract thought. The list of problems we have mentioned does not include all the most important problems, and nor are the problems mentioned all of the greatest importance. And towards the end of this book, the problems we have discussed are almost incomprehensible. With the exception of a few deceptively innocent problems, the great mathematical problems of today are conceived by and for experts. There are problems in all fields – graph theory (strong perfect graph theorem, solved; Happy Ending problem, unsolved); linear algebra (Hadamard matrix problem, unsolved); function theory (Collatz conjecture, unsolved); number theory (196-algorithm problem, and is 10 a solitary number?, both unsolved); probability (generators of symmetry groups problem, unsolved); fluid dynamics (percolation threshold problem, unsolved); encryption (Dorabella Cipher, unsolved); group theory (inverse Galois problem, unsolved); game theory (angel problem, unsolved), and so on and so forth.

There are many problems, but even more numerous are the neurones dedicated to solving them, and not even Gödel, in his theses on the limits of proof and computation, has managed to delimit mankind's facility for deduction. It may be true that there are statements that can never be proved, but there is nothing to stop us proving that a statement is unprovable.

Bibliography

Cipra, B., *What's Happening in Mathematical Sciences*, 7 vols., American Mathematical Society, Providence, 2006.

Courant, R., Robbins, H., *What Is Mathematics?,* ed. Ian Stewart, Oxford University Press, Oxford, 1996.

Du Sautoy, M., *The Music of the Primes*, Fourth Estate, London, 2003.

Devlin, K., *The Millennium Problems*, Barnes and Noble, New York, 2006.

Dunham, W., *Journey to Genius: The Great Theorems of Mathematics*, Penguin, London, 1991.

Jacobs, H., *Mathematics: A Human Endeavor*, W.H. Freeman, New York, 1982.

Roman, M., *Symmetry and the Monster*, Oxford University Press, Oxford, 2006.

Singh, S., *Fermat's Last Theorem*, Fourth Estate, London, 1997.

Yandell, B.H., *The Honors Class: Hilbert Problems and Their Solvers*, A.K. Peters, New York, 2002.

Index

Abel, N. 72
Aitken, A.C. 9
Aleph 105
algebraic geometry 113, 129, 131, 148
algorithm 86-87, 110, 114, 128-129, 148
angle 17-21, 66
anomaly 46
Appel, K. 87, 90
Archimedes 12, 18-20, 19-31, 108
area 11-12, 29-31, 33, 38, 46
Aristarchus de Samos 44
Arnold, V. 112
Artin, E. 110, 114
axiom 106-107, 108
    of Zermelo-Fraenkel 97, 107

Basel problem 48-52
beal, A. 95
Bernoulli 33-35, 48-49, 56
Bernstein, S.N. 116
Bieberbach, L. 94-95, 115
binary, system 27
Birch, B. 148, 150
Bolibruch, A. 119
brachistochrone 36
Brahe, T. 44-45
Branges de Bourcia, L. de 95
Brun, V. 94

Cantor, G. 104-106, 111
Cardano, G. 20, 70-71
cardinal 104-105
Catalan, E. 98
cathetus 21
Chaitin, G.J. 139
Chen Jing-Run 54, 56, 59
Chen Ning Yang 144-145
class 102-104, 126, 129-131
Clay
    Mathematics Institute 9, 54, 109, 121-122, 129, 131, 132, 145
    problems 121-150
coefficient 15, 69, 110, 112, 114, 129
Cohen, P. 106-107
cohomology 113, 129, 131
compact 134, 137, 145
computer 42
computer 42, 90-91, 93, 125-129, 147
conic 31
conjecture
    four colours 87-90
    Goldbach's 52-56, 59
connected 149
constant 12, 51, 54, 78-79, 92, 144
Conway, J.H. 69, 79
Cook, S. 124
coordinate 36, 48, 55, 119, 124
Copernicus, N. 44-46
coplanar 57
cosine 69
countable 104
cuboid 61-63
cycloid 32-37
cylinder 29-31

Davis, M. 110
decimal 14, 49, 78
decision 110, 124, 126
Dedekind, R. 84
Dehn, M. 108
Del Ferro, S. 69-71
Deligne, P. 131, 139
Delos 15-16
density 39-41, 55, 91
diagonal 21, 22, 61, 98
diameter 12
differential
  calculus 31, 47, 51
  equation 22, 48, 56, 118-119
  form 130
dimension 40-41, 115-116, 131-137
distance 23, 31, 48, 64, 86, 146
divisor 23, 25, 28, 124, 144

edge 16-17, 62-63, 133
Elements 9, 22-23, 27, 66
Elkies, N. 84
ellipse 46
epicycle 44-45
equation 40, 61, 69-73, 146-149
  Diophantine 61, 84, 110, 148
equivalence relation 102-103
Euclid 9, 11, 22-28, 66-67
Eudoxus of Cnidus 12, 30
Euler, L. 13, 27, 43-79, 81, 84, 139-140
exhaustion 12, 30

factor 24-27, 84, 95, 124, 143, 149
factorial 73, 86
Fedorov, E. 115
Fermat, P. 67-68, 81-85, 95, 97
Ferrari, L. 70-71
field 17, 56-58, 111, 139, 148
Fields 83, 131, 132, 137, 138, 149
Fior, A.M. 70
focus 45
fractal 10, 55
Freedman, M. 137
Fuchs, L. 119
function 76, 85, 94, 112-120, 124, 142-144, 149
  analytic 116, 118
  divisor 25, 27, 144
  holomorphic 94
  zeta 51, 76, 79, 139-141, 143, 149

Galilei, G. 34
Galois, É. 72-73, 151
Gauss, C.F. 66-68, 75-76, 110, 141
Gelfond, A. 109
geodesic 108
Germain, S. 84
Giorgi, E. de 116-117
Goldbach, C. 52-56, 59
graph 65, 86, 87, 89
  Hamiltonian path 86, 123-124
Grothendieck, A. 131, 132
group 72-73, 108, 115, 119, 136, 144-145, 149
  gauge 144-145
  Lie 108, 145
Guthrie, F. 89
Guy, R. 63, 79
Gödel, K. 106-107, 110, 139, 151

Hadamard, J. 76, 151

Haken, W. 87, 90
Hales, T. 38, 42
Hamilton, R. 137-138
Hamiltonian circuit 86, 123-124
Hardy, G.H. 91-92, 138
Hasse, H. 111
Heawood, P. 89
Heesch, H. 89, 116
heliocentric 44, 46
hexagon 38
Hilbert, D. 77, 81, 101-120, 121, 148
Hodge
  class and conjecture 129-131
  Hodge, W.V.D. 130-131
homeomorphism 134
Huygens, C. 37
hypotenuse 21
hypothesis
  Continuum 101, 106-107
  Riemann 76-77, 95, 109, 138-144

infinity 23-25, 28, 84, 104-105, 139
integral 31, 50, 76, 118
invariant 85, 113
isohedral 115-116

Kempe, A. 89
Kepler, J. 38-42, 44-48
Kintali, S. 59
Koebe, P. 120
Kolmogorov, A. 112
Kronecker, L. 111-112
Kummer, E. 84
Königsberg 63-66

Ladyzhenskaya, O. 148
Lagrange, J.L. de 57-58, 71, 114
Lamé, G. 84
Landau, L. 59
Landry, F. 68
Legendre, A.M. 58-60, 75, 84, 109
Leibniz, G.W. 36, 49
limit 13, 30-31, 54, 75, 78
linear combination 17, 129-130
linear programming 42
Liouville, J. 73
Littlewood, J.E. 91-92
logarithm 75, 78
Lovelace, A. 28

magic square 99
manifold 113, 119, 131, 133-137, 144
Mascheroni, L. 78
Matiyasevich, Y. 110, 148
matrix 98
Maxwell, J.C. 144
mechanics 30, 45, 48, 125, 139
Menger, K. 86
Mengoli, P. 49
Mersenne, M. 27-28
Mihailescu, P. 98
Mills, R. 144
modular form 85
monodromy 118-119
Morgan, A. de 89
multiple 73, 84
Möbius 142

Nagata, M. 113
Nash, J.F. 117, 138
Navier, C.L. 147
Newton, I. 11, 17, 36, 47-48, 56
Nicely, T. 90, 93
NP-complete 128
number
  algebraic 15, 69, 79
  amicable 28-29
  complex 51, 69, 85, 109, 120, 131, 139
  composite 23-25, 27, 67, 73-74
  constructible 15, 17, 20
  ideal 84
  integer 22, 52, 54, 61, 78, 81, 90, 111
  perfect 26-27
  prime 23-28, 52-60, 67-78, 90-99
  rational 22, 61, 79, 111, 148
  semiprime 54, 59
  Skewes' 77
  transcendental 15, 51, 79, 109
  twin prime 59, 73, 90-94
  orbit 44-47, 56-58, 115
  oval 113

packing 39-41, 116
Pappus of Alexandria 37
partial derivative 118, 147
Perelman, G. 122, 132, 138
period 9, 32, 46, 73, 149
permutation 72
planet 43-47, 56, 58
Poincaré, H. 57, 120, 122, 132-138
polygon 13, 38, 66-69
polyhedron 47, 115-116, 123
polynomial 49, 67, 69, 83, 110, 112, 114
polynomial time 126, 128
prism 37-38
Putnam, h. 110
P versus NP 86, 123-129
Pythagoras 21-23, 25, 61
Pólya, G. 115

quadratic 110
quadratic integers 84
quark 144-145
quartic 71, 77
quintic 71

reciprocity 109-110
reflexive 102
Reinhardt, K. 116
Ribet, K. 85
Ricci flow 137-138
Riemann, B. 51, 54, 76, 119, 138-144
Robinson, J. 110
root 73, 112
Ruffini, P. 72
ruler and compass 15-18, 20, 66, 68-69
Russell, B. 97, 106

Schneider, T. 109
Schnirelmann, L. 54
Schubert, H.C.H. 113
segment 20, 54
series 17-18, 23-24, 49-50, 73, 77, 94, 105
  Taylor series 49, 149-150
set 72, 97, 101-107, 124-128, 137

Shimura, G. 85
Siegel, C. 111
Simó, C. 58
sine 20, 66
singularity 57, 118-119
Smale, S. 137
solvable 73
space 23, 39, 105, 115, 133, 141
sphere
    celestial 44, 47
    geometric shape 29-31, 38-41, 116, 133-138
squaring 11, 13, 15
statistics 79
Stokes, G.G. 147
Stäckel, P. 90
Sundman, K.L 57
Swinnerton-Dyer, P. 150
symmetrical 102

Tait, P.G.. 98
Taniyama, U. 85
Tartaglia (Fontana, N.) 70-71
tautochrone 36-37
Taylor, R. 82
tetrahedron 108
Thurston, W. 137-138
tiling 37-38, 115-116, 126
topology 65, 114, 130, 134
torus 134-136
transfinite 104-105
transitive 102
triangle 21, 57
trigonometry 20
trisection 20
Turing, A. 125-126
Turing machine 107, 125-127

Ulam, S. 60
uniformisation 119-120

Vallée Poussin, C. de la 76, 138
variations 34, 35, 116, 118, 120
vector 118
Vinogradov, I. 54, 78
volume 16, 29-31, 39, 108
Von Lindemann, C.L.F. 13, 15

Wantzel, P. 16, 20
Waring, E. 77-78
Wiles, A. 81-83, 85, 97, 150
Witten, E. 145-146

Eternal Challenges

The great conundrums of mathematics

What constitutes a relevant problem in mathematics? This volume attempts to provide an answer to this question, exploring dozens of intriguing conundrums. Some of them appear to be complicated but turn out to be simple, while others, which at first glance seem to be very easy, are much more challenging. The book provides an eye-opening history of mathematical problem-solving through examples that have obsessed mathematicians throughout the ages.